

A COMMON APPROACH TO EXTENDING COMPUTER SECURITY  
CONCEPTS TO THE UNIVERSAL DISTRIBUTED  
NON-TRUSTED ENVIRONMENT

Approved by :

\_\_\_\_\_  
Dr. James George Dunham

\_\_\_\_\_  
Dr. Eric Hall

\_\_\_\_\_  
Dr. Alireza Khotanzad

\_\_\_\_\_  
Dr. Richard Levine

\_\_\_\_\_  
Dr. David Matula

A COMMON APPROACH TO EXTENDING COMPUTER SECURITY  
CONCEPTS TO THE UNIVERSAL DISTRIBUTED  
NON-TRUSTED ENVIRONMENT

A Praxis Presented to the Graduate Faculty of the  
School of Engineering and Applied Science  
Southern Methodist University

in

Partial Fulfillment of the Requirements

for the degree of

Doctor of Engineering

with a

Major in Electrical Engineering

by

Richard Dan Herschaft

(B.S.E.E., The University of Texas at Arlington, 1984)  
(M.S.E.E., Southern Methodist University, 1986)

December 17, 1994

COPYRIGHT 1994

Richard Dan Herschaft

All Rights Reserved

Herschaft, Richard Dan      B.S.E.E., The University of Texas at Arlington, 1984  
M.S.E.E., Southern Methodist University, 1986

A Common Approach to Extending Computer Security  
Concepts to the Universal Distributed  
Non-Trusted Environment

Advisor: Associate Professor James G. Dunham

Doctor of Engineering degree conferred December 17, 1994

Praxis completed December 15, 1994

Computer security involves internal controls and external controls. As a computer system grows distributively, the environment in which it exists can become less trustworthy. Less reliance can thus be placed on external controls, such as locked rooms. In the extreme, a highly distributed computer system operates on a worldwide scale. Information transfer exists between users, autonomous to varying degrees, where the only certain link is some form of communications channel from one user to another. The term distributed is appropriate since by each computer carrying out its own information processing needs, society as a whole is able to function.

Although parties involved with information have a self-centered aspect, their actions result in a communal effort of information generation, where a unit of information is generated by one party and passed to another for regeneration. This process can trace out simple to complex paths. Along the way each party has rights in the information stemming from its role as "author" and user. Concern for these rights arises from the private or proprietary nature of information. In order for information transfer to be made efficient, the rights to information should be made a part of the informational unit, both technically and legally. As information traces its path, each author can add to the restrictions placed on the use of the information, and each user is constrained by the system to abide by these restrictions.

This paper describes this universal computer system and devises a secure framework for it by expanding upon computer security concepts which were previously devised for a more limited environment. This architecture relies on the internalization and further systematization of external controls. The computer security concepts that are extended to work in this environment are the security watchdog, the access control list, and public key cryptography with its certification authority. Also developed are the concepts of a tamper proof device, a device validation authority, and the policy concerns regarding the mutual agreement over the formulation of an access control list. The result is a design which can effectively accomplish information security in the environment of the everyday world.

## TABLE OF CONTENTS

LIST OF FIGURES .....	xi
LIST OF ACRONYMS .....	xiii
CHAPTER	
1. INTRODUCTION .....	1
1.1 Introduction .....	1
1.2 Private and Proprietary Information Property .....	2
1.2.1 The Effect of the Computer on Information Misappropriation .....	3
1.2.2 Private Transactional Information .....	4
1.2.3 Proprietary Information .....	6
1.3 Basic Objective of Proposed Technical Solution .....	6
1.3.1 Extensions to Computer Security Concepts .....	7
1.3.2 Basic Design .....	9
1.4 Background .....	16
1.5 Overview of Threats and Countermeasures .....	19
2. THE INFORMATION PROTECTION TAG .....	26
2.1 Introduction .....	26
2.1.1 Information Usage States and Influences .....	26
2.1.2 The Information Access Control List .....	29
2.2 A Selection of Groupings of Usage Influences .....	32
2.3 The Data Base of Usage Influences .....	35
2.4 Attribute Categories of the Information Distribution Directory .....	37
2.4.1 Syntactical Attribute Category .....	37

2.4.2	Naming Attribute Category .....	38
2.4.3	Informational Attribute Category .....	48
2.4.4	Controlling Attribute Category .....	48
2.5	Sections of the Information Protection Tag .....	53
2.5.1	Identifying Information Section .....	54
2.5.2	Originators Link Section .....	55
2.6	The Protected Information Unit .....	59
2.7	Abstract Syntax Notation One to Define the IPT .....	60
2.7.1	Brief Background on ASN.1 and its Encoding .....	61
3.	COMMUNICATIONS BETWEEN DEVICES .....	64
3.1	Introduction .....	64
3.2	Public Key Cryptography for Secure Communications .....	64
3.3	Aspects of Secure Communication .....	65
3.3.1	Data Confidentiality .....	66
3.3.2	Data Integrity .....	66
3.3.3	Non-repudiation .....	68
3.3.4	Access Control .....	69
3.3.5	Peer Entity Authentication .....	69
3.4	Authentication of the Receiving Device .....	70
3.4.1	The Importance of Valid Device Credentials .....	70
3.4.2	The Certificated Token .....	71
3.4.3	Access Rights are Device Centered .....	73
3.4.4	Validated Usage Influences Belong to the Device .....	74
3.4.5	Validation of Usage Influences at a Device .....	74

3.4.6	Considerations for Selecting the Time Period of Validity of a Usage Influence .....	76
3.4.7	Examples of Usage Influence Validation Techniques .....	78
3.4.8	Transfer of Device Credentials from Receiving to Sending Device .....	85
3.5	The PIU's Place in the Open Systems Interconnection Reference Model .....	86
3.5.1	OSI Basic Architecture .....	87
3.5.2	The IACL at the Application Layer .....	88
3.5.3	The IACL at Other Relay Layers .....	90
3.5.4	Encryption in the OSI Model .....	92
3.6	Attaching a Protection Tag to Protected Information .....	93
3.6.1	Attachment Using the Processor Channel .....	94
3.6.2	Devices Require Information Watchdog .....	97
3.6.3	Input Control Needs are Similar to those of Output Control .....	98
3.6.4	Connectionless and Connection-oriented Transactions .....	98
4.	THE INFORMATION WATCHDOG .....	101
4.1	Information Protection at a Device .....	101
4.1.1	Internal Controls .....	102
4.1.2	External Controls .....	104
4.1.3	Current Systems at Risk .....	104
4.2	External Controls for Watchdog Resident Devices .....	106
4.2.1	A Design for Built-in Physical Security .....	106
4.2.2	Compliant Devices and Modularity .....	108
4.2.3	System Survival in a Compromised Device Environment ..	109



4.3	Internal Controls for Watchdog Resident Devices -- The General Purpose Computer .....	113
4.3.1	Information Management .....	115
4.3.2	Device Management .....	117
4.3.3	Memory Management .....	120
4.3.4	Processor Management .....	127
4.3.5	Recap of Changes Needed to Systems Software .....	129
4.4	Internal Controls for Watchdog Resident Devices -- Other Processing Architectures .....	131
4.4.1	Multiple Information Watchdogs in a Single Device .....	131
4.4.2	Information Watchdogs in Multiple Devices .....	132
4.4.3	Simple Devices .....	134
4.5	Examples of System Use .....	134
4.5.1	Control of Flow and Access of Information .....	134
4.5.2	Compensation for Use of Software Product by End User ..	137
4.5.3	Transfer of Music to a Compromised Device .....	139
4.6	Adding Functionality to the Information Watchdog .....	140
5.	CONCLUSION -- PATHWAYS TOWARD GENERAL ACCEPTANCE AND TASK PLANNING FOR SYSTEM DEVELOPMENT .....	142
5.1	Pathways Toward General Acceptance .....	142
5.2	Task Planning for System Development .....	145
5.2.1	The Information Distribution Directory .....	147
5.2.2	Biometric Technology .....	147
5.2.3	Encryption Techniques .....	147
5.2.4	Outer Casing of an IW Protected Device .....	148
5.2.5	Inner Casing of an IW Protected Device .....	148

5.2.6	Controlled Manufacturing . . . . .	149
5.2.7	Compliance with Environmental and Quality Standards . .	149
5.2.8	Operating System of an IW Protected Device . . . . .	149
5.2.9	Electronic Hardware Design . . . . .	150
5.2.10	Information Usage Influence Verification: Location . . . . .	150
5.2.11	The Model of Information Flow . . . . .	151
APPENDIX		
A.	HIGHLY TRUSTED INFORMATION SYSTEMS . . . . .	155
B.	THE INFORMATION PROTECTION TAG STRUCTURE . . . . .	169
REFERENCES . . . . .		173

## LIST OF FIGURES

Figure	Page
1.1. Sequential steps to establish system and transfer information .....	15
2.1. The Organizational Unit hierarchical usage grouping .....	38
2.2. The Organizational Position grouping of usage influences .....	41
2.3. The Work Related Role grouping of usage influences .....	43
2.4. The Device Type grouping of usage characteristics .....	50
3.1. OSI Seven Layer Architecture .....	88
3.2. Dual channels aid with the conduction of transactions including the attachment of the protection tag to the generated information .....	97
4.1. The Hierarchical Domain Architecture is based on the trustworthiness of groups of software .....	102
4.2. The Information Watchdog is implemented within the four resource managers of an operating system .....	114
4.3. Protected Information Memory Access .....	120
4.4. Memory Management: 1st Phase of Context Switch .....	122
4.5. Memory Management: 2nd Phase of Context Switch .....	123
4.6. Example of Memory Management .....	124
4.7. Example of steps to control flow and access .....	135
5.1. Time line of critical path for system development .....	153
A.1. Hierarchical Information Processing Topology .....	159
A.2. An information service should be factored into separate processing activities .....	164
A.3. A model of how a PIU is generated and how it may be transferred .....	165

A.4. Alteration to applicable branches of the previous model to allow for an HTIS .....	166
A.5. Alignment of sectors of representational disk packs for two clients within the same or different HTISs .....	167

## LIST OF ACRONYMS

- AAC** Activity Anonymous Code. Part of an HTIS, it is a code which relates AIUs within the same topologic ring. It integrates activities which are part of the same client service.
- AIU** Activity Information Unit. A unit of information formulated by an HTIS in accordance with the principles of topology, aggregation, and stationarity. The aim is to better control information availability by creating units of information to which tighter fitting access control lists can apply.
- ASN.1** Abstract Syntax Notation One. From CCITT Recommendation X.209 [3], ASN.1 (X.208 [2]) "specifies a notation for the definition of abstract syntaxes, enabling application layer specifications to define the types of information they need to transfer using the presentation service."
- CA** Central (Certificating) Authority. The authority which oversees the content of the IDD and its corresponding information usage influence validation techniques. The structure within the CA can be decentralized.
- DAT** Device Authentication Token. Contains a device's credentials in the form of certificated usage influence tokens, as well as the public key of a device. A receiving device must (directly or indirectly) submit a DAT to a sending device before it can receive a PIU.
- HTIS** Highly Trusted Information System. A system of services offered by an organization where the information protection approach for each service revolves around each client.
- IACL** Information Access Control List. It is a list of recipients (usage states) that have permission to receive logically associated protected information. It is a section of the IPT.
- IDD** Information Distribution Directory. A universally accessible data base which contains the commonly identified information usage influences along with various associated attributes.
- IMAT** Information Memory Assignment Table. A table used to determine the PIMA that a memory address is located within.
- IPT** Information Protection Tag. It contains instructions to direct the actions of an IW in handling logically associated protected information. It is a section of the PIU.

- IW Information Watchdog. A class of standard components which carry out the instructions in an IPT. A device compliant with the protected information environment, depending on its architecture, is required to have one of the IWs as part of its operating system.
- IWD Information Watchdog (protected) Device. A device which contains an IW and which is designed and manufactured according to rules specified to make the device tamper proof.
- LC Least Common. An IACL which has been formulated, by an information management function, from IACLs which are to be opened for reading at the same time. The LC IACL contains the common recipients across all the opened IACLs.
- PAAT PIMA Access Allowed Table. A list of PIMAs that are allowed to be accessed at a given time.
- PIE Protected Information Environment. A system which secures the transfer of private and proprietary information in a distributed non-trusted environment. It primarily involves the transfer of PIUs between information watchdog resident devices.
- PIMA Protected Information Memory Area. An area of memory, contiguous or dispersed, physical or virtual, to which an LC IACL has been assigned. The assigned LC IACL is used to determine to which PIUs the contents of the memory may be written.
- PIU Protected Information Unit. A generic term for a protected instance of a data structure. It can apply to frames, packets, records, files, etc. for which an originator has decided to have protected information controls apply. It mainly consists of an IPT and protected information.
- SI System Information. Information existing within an HTIS which is not directly indicative of a client. The format is non-specific.
- TAC Transaction Anonymous Code. Part of an HTIS, it is a code associated with an AIU which relates it to a more complete parent AIU within an inner ring. It can be used to hide items of information including the identity of a client engaged in a specific transaction.

# CHAPTER 1

## INTRODUCTION

### 1.1 Introduction

The title of this paper is A Common Approach to Extending Computer Security Concepts to the Universal Distributed Non-trusted Environment. The qualifying terms in the title are intended to show the scope of the subject but ambiguity may still remain. Therefore each term is now discussed:

- "Common Approach" means that the technical solution should be applicable without significant modifications to a broad class of related problems.
- "Extending Computer Security Concepts" means that various computer security concepts that may be considered to already exist in some form are further developed to apply to the environment of interest. Only those concepts that will be altered or specifically applied to the new environment will be discussed; other concepts may be relevant as part of a complete design but will not be discussed.
- "Universal Distributed Non-trusted Environment" refers to information usage on a worldwide scale where each information user may be autonomous both in technical configuration and administratively from other users with the only certain link being some form of communications channel to another user. The term distributed refers to the big picture of the worldwide computer network, where by each computer carrying out its own information processing needs, society as a whole is able to function. This environment may more simply be described as the everyday world. This environment is considered to be a superset of the limited trusted environment, to which the techniques developed should also be applicable.

To these qualifying terms can be added -- with the aim of protecting private and proprietary information -- to show the desired outcome of the technical solution. This category of information can be interpreted quite broadly but is meant to imply something less than information pivotal to the outcome of national crises. This influences the level of achieved security as well as the security features offered. The distinction between private and proprietary information and the increasing need to be concerned with their protection is discussed in the next section.

### 1.2 Private and Proprietary Information Property

The concern that an owner of private information has is that its use not adversely affect him. The concern that an owner of proprietary information has is that he be rewarded for each use of the information. Both require that information distribution be restricted. The difference in compromise associated with each of these types of information may be one of quality versus quantity. A single usurpation of private information into the wrong hands may destroy its value to its owner; each usurpation of proprietary information may simply deprive its owner of another unit of value. Value in terms of proprietary information usually means monetary value; value in terms of private information can mean monetary value or an intangible quality such as reputation. This is not so different from other classes of property which can have monetary as well as intangible value, i.e., a family heirloom. In terms of the business world, trade secrets would be considered private information while a data base for sale would be proprietary information. Individuals usually are concerned with the intangible value of private information which may or may not have financial implications. A large fear is that the available body of recorded information on a person may substitute for a person's characteristics as expressed in a more personal or current manner. Additionally the recorded information may be incorrect. A connection exists between private information



and proprietary information -- individual instances of private information may have insignificant value but when gathered and arranged may increase in financial value, thus encouraging a transformation of private information into proprietary information.

### 1.2.1 The Effect of the Computer on Information Misappropriation

Information is a form of property. As with any item of property, the degree to which it may be misappropriated is based on the value of the information and the ease with which it can be misappropriated. As a property group, more information can be misappropriated if there is more of it in existence. Computer technology has facilitated all of these factors.

- Information has been made more valuable due to the ease with which it can be processed. Processing can reveal insights in information or can handle information in a production line manner by producing such outputs as addressed envelopes. The computer acts as a front end to human abilities where otherwise the type and amount of information would cause an overload condition. The technical concepts discussed in this paper will lose their effectiveness as the content of the involved information becomes simpler in terms of human manipulation and comprehension. At the extreme end of simple human comprehension, gossip will hardly be affected at all.
- Information can be more easily misappropriated due to the ease with which telecommunication networks can transport it and due to the various available media for the output of data. Telecommunications networks are offering greater bandwidth and greater connectivity of diverse systems. Information has also been easy to misappropriate because owners of the information have not been safeguarding their claims to it. Just as the title to land that is not protected can pass into the hands of squatters, the same can and does happen to private

information. Some mechanism is needed for information originators to lay claim to, as well as to secure, private and proprietary information.

- Information in digital form is also becoming more available as a result of the positive trend in performance to price of software and electronics and the increasing portability of information related equipment. Due to the functional advantages of the telephone, word processor, point of sale terminal, etc., human interaction increasingly is either accompanied with or transpired using digital communications. The increasing degree to which human interactions are being reduced to a bit stream, poses an increasing privacy threat.

### 1.2.2 Private Transactional Information

Some information is already protected by law or by contract under law such as through copyrights or nondisclosure statements. Usually in these cases, the information (or its physical manifestation) is generated with the direct intention of being offered for sale. The information may very well have not been generated in the first place if a means to claim ownership was not available. Much private information is generated as a by-product of the need to complete transactions. Businesses as well as individuals are at jeopardy of having their private information usurped in this manner.

#### 1.2.2.1 Characteristics of Transactional Information

The characteristics of information which determine how it can be used for purposes consistent with the owner's desires, also determine how the information can be used when misappropriated. Transactions can be classified as generating computer intelligible information or computer non-intelligible information. Computer intelligible information consists of symbols or numbers from which the computer can discern meaning. Computer non-intelligible information can as well be numerically manipulated but doing so does not lead to its being related in a significant way to an external idea. Over time, as computers are becoming more "intelligent", non-intelligible information

is becoming intelligible information. The line between computer intelligible and computer non-intelligible information presently occurs in the area of free-form information, such as natural human speech in a conversation. Telephone conversations have traditionally been an area for the invasion of private information through the use of the wiretap. The information derived from a wiretap can be understood by a computer to the degree that it can recognize key words. As artificial intelligence methods develop, free-form information may become understandable so that the contents can be categorized.

The protection of computer non-intelligible private information can also be assaulted by developing computer technology. Such information possibly originated as an analog signal can be converted into a bit stream. Digital information can easily be stored and duplicated using computer technology and transmitted using digital telecommunications networks. The increasing capacity of memory, storage media, and telecommunications channels along with compression technology will allow for the more cost effective use of computer non-intelligible information -- a greater misuse of private information may accompany this. Computer non-intelligible information is usually human intelligible and so may hold value if presented in conjunction with processed computer intelligible information.

#### **1.2.2.2 Control Over Transactional Information**

Although the distribution of private information generated as a secondary outcome of a transaction may seem inevitable or inconsequential to some parties to a transaction, other parties to the transaction may purposefully influence the information generated and its distribution. These parties have control over the information generating apparatus. There are a number of reasons for this imbalance in processing control. Due to the marginal value of information, the party that needs to invest in computer technology to carry out the transaction may be the party that controls the information exchange. For instance, in a retail environment, the vendor requires, for all

practical purposes, a point of sale terminal to consummate the transaction. The computer technology may be bulky or just inconvenient to transport, and so only the stationary party can make use of computer processing power.

As described later, all parties to a transaction are owners of the information with valid uses for the information. For each party to have an equal say in the disposition of the information, each party needs computer power dedicated to looking after its interests.

### 1.2.3 Proprietary Information

Although means exist for owners of proprietary information to claim their ownership right, changing technology may allow for the uncontrolled distribution of their information. For instance, the photocopy machine allows for the easy copying of copyright protected literature. As more information (music, literature, video) is stored in a digital format in computer systems, the output mechanisms, whether on hard media or over a telecommunications network, allow for the easy bypass of law abiding behavior. The same technology that can be used to claim and protect private information can be used to claim and protect proprietary information. In addition, the authors and users of proprietary information are generally the same as the "authors" and users of private information. Therefore, the same system can be used for both, allowing the developmental and implementation expenses to be spread over more benefits.

### 1.3 Basic Objective of Proposed Technical Solution

What this paper is trying to accomplish, in terms of a technical solution to protect private and proprietary information, can be explained using an analogy. The analogy makes use of the contribution of the microprocessor. Just as the microprocessor extended CPU concepts to a specialized environment, that of a single integrated circuit, this paper will extend computer security concepts to the universal distributed non-trusted environment (the everyday world). The microprocessor may be based on general CPU

concepts, but the IC environment influences the design in unique ways and may require that concepts be tailored for the environment. The same is true for computer security concepts in regards to the environment of the everyday world. Counter to the environment of the everyday world is a limited environment.

### 1.3.1 Extensions to Computer Security Concepts

Assuming that most computer security concepts are geared to a limited environment, where limited environment generally refers to a formal organization, the following are some of the extensions that can be made to computer security concepts so that they can apply to the everyday world:

- In a limited environment, a certain degree of trust can be expected of all people who have administrative control over the physical security of a computer system. Assuming that the security system doesn't have any holes, the users can effectively be limited to permitted operations. In the everyday world, information may need to be sent to diverse computer systems for limited processing. The users may not be trusted to restrict their processing to the limited degree allowed. This problem can be solved by requiring in compliant processing devices a common security component controlled by the received information -- an information watchdog -- and by making it tamper proof.
- In a limited environment, the designations in an access control list can be simple. For instance, the military has unclassified, confidential, secret, and top secret; a commercial computer may have work groups and user IDs. The relationships of entities in the everyday world are very complex and so these relationships need to be understood in order to form precise (as well as concise) access control lists.
- In a limited environment, it can be relatively easy for a person generating information to find out the designations, in terms of spelling, syntax and semantics, which he wants to include in the access control list associated with the information. The everyday world requires a universally accessible data base of

entity designations. The concepts described in CCITT X.500 [1] can be applied to this need.

- In a limited environment, the policy governing which entities should have access to certain information, that is which designations should go into an access control list, is usually straight forward. This is because in a formal organization, decisions in general can be made by some position within an organizational hierarchy. In the everyday world the policy making governing this can be very complicated. In terms of private information generated in a transaction, many parties may be involved, each with self interests that may be in conflict with the self interests of others. How can this bargaining process be streamlined with technology so that the conduction of transactions is not hindered?
- In a limited environment, the designations in access control lists, in terms of syntax, are simple. A "fixed" format can be used to code this label information. The format of the label for the everyday world must be flexible so that it can contain various types of directions, including optional directions. Abstract Syntax Notation One (CCITT X.208 [2], X.209 [3]), or a similar language, can be applied to form a flexible access control list label.
- In a limited environment, trust can be placed in an administrator to assign the appropriate designations to users. This is needed so that the designations in an access control list associated with information will be adhered to. In the everyday world this administrative function still needs to be performed but of necessity must be accomplished in other ways. Some equipment, limited to performing certain functions, may be able to be sold with a preconfigured security label. Other cases may require an independent verification process in order to determine the appropriateness of labels assigned to entities. This

validation can then be indicated by the cryptographic signature of an entity's label.

Each of these listed items is cited at the place within this paper where the need and its possible solution are further developed.

### 1.3.2 Basic Design

The computer security concepts to be extended relate to one another and these relationships influence how a security concept should best be implemented. Therefore computer security concepts will be discussed in the context of a design.

The design makes use of the above listed extended computer security concepts as well as computer security concepts in existing designs to protect private and proprietary information as it naturally flows -- from originator to user through possibly many intermediaries (each intermediary being a possible modifier and user as well). Alternative, but unacceptable, information flow patterns could have all information first sent to centralized data bases for further distribution allowing only two data paths -- from originator to data base and from data base to user. Alternatively the originator could act as the central data base for his own information allowing only a single data flow path -- from originator to final user. These centralized approaches do not take into account the value added to information as it passes from one user to another. A modified centralized approach that would require that all processed information pass back through the originator could cause a bottleneck to its distribution. Also since all parties involved with the generation of information are its originators, a centralized scheme would require the cooperation of all originators to allow for the further distribution of processed information.

To uphold the information user's rights, once rights to information are given they should not be taken away. Therefore, rights to information should be formulated and placed in an information protection tag when the information is originated; after that the information is on its own in the sense that it can pass from user to user as long as each

transfer is in agreement with the associated information protection tag. A specialized component in each receiving device will make sure that the rights to the information as specified in the information protection tag are followed.

### **1.3.2.1 Basic Principles**

Some of the basic principles of the design are:

- Access Control List -- An information protection tag accompanies all information that is to be protected by the proposed system. The information protection tag implicitly and explicitly gives instructions on:
  - what usage states (discussed next) can receive the information
  - what processing constraints should be maintained at a usage state
  - whether or not a communications link must be established between a device possessing protected information and an originator of the information. This can entail an audit message sent to an originator of information before information is transferred or output.
- Standard Representation of Information Usage Universe -- A usage state indicates the existence of conditions at a device which can influence the way information is used. A usage state must have a commonly understood meaning so the designation of a usage state must be based on established rules. Usage states are made up of usage influences and these are listed in a universal data base. An instance of a usage state is a particular person using a particular program. The person and program are each usage influences. A device can have many usage states or a particular device may always operate in the same usage state.
- Information Watchdog -- Each device which is to receive private or proprietary information must have an information watchdog (all the possible usage states of a device share the same information watchdog). The information watchdog's role



is to make sure that the instructions in the information protection tag accompanying any information that the device receives are carried out. Since the information watchdog must always be in control of protected information, all communication of protected information between devices must occur between information watchdogs. Since some form of the information watchdog must be in all compliant devices, it may be required in diverse information processing devices, from supercomputers to label printers. The information watchdog component must be tamper proof. This in turn requires special construction of the device in which the information watchdog resides.

- Public Key Cryptography -- In order to keep information traveling between information watchdogs secure, a public encryption key should be associated with each watchdog and should be used (along with a symmetric scheme) to encrypt transmitted information destined for a watchdog. Ideally the private key used to decipher the information should only be known by the destination watchdog (and not any human including the owner of the device).

Therefore, the environment of the everyday world can be modeled as a network of nodes, where information and associated rights flow between nodes. The design described in this paper aims at making this network a closed system. Information flow between nodes is made secure with cryptography. At a node, information processing, which occurs within a device, is made secure from external threats with built-in security construction techniques, and from internal threats with the control afforded by an information watchdog. Information flow and access rights within this closed system can be directed with access control lists which are formed based on a flexible and meaningful representation of information usage.

### **1.3.2.2 Finer Principles**

Transfer access and read access of a unit of protected information are permitted when a usage state in a receiving device's credentials matches a usage state in the

information access control list (IACL) associated with the unit of protected information (the IACL is part of the information protection tag). The matching process is performed by the information watchdog. For transfer access the match is performed at the sending device. For read access the match is performed at a device which is in possession of protected information. The validity of each information usage influence which comprises a particular device's credentials is determined on a periodic basis by (primarily automated) procedures which are administered by independent trustworthy organizations.

The proposed approach to protecting privacy can be applied to any information system in terms of the function to be performed. The system in terms of its mechanism must allow a digital information protection tag to be associated with units of information (the units of information are also to be digital although the concepts may be extendable to analog signals). The information protection tag is physically or logically part of the informational unit and is usually generated in conjunction with (often preceding) the generation of the information. In terms of the transfer of information, an information protection tag is associated with a one-way flow of information but a two-way or multi-way flow can be accomplished by supplying each flow direction with the same information protection tag -- where the information goes, the protection tag goes.

Also the size of the information unit is unimportant as long as the information watchdog at each device which processes the information can maintain the integrity and confidentiality of the information - excess bits can not be stored beyond the control of the information watchdog. Therefore channels and processing equipment that are involved with telephone conversations, fax transmissions, the physical transfer of information on a diskette, and the transmission of packets on a data network are all examples of systems to which this approach can be applied.

An information protection tag is to be associated with all the information related to a transaction. A transaction can vary from a single event to a series of ongoing

events. It is distinguished by a constant information protection tag which is mutually agreeable to all the parties involved. The information in a transaction can be allotted to protected information units (messages) by each party independently of all the other parties. The contribution of each party derives its informational value from its relations to the contributions of the other parties, as in a telephone conversation, so the information protection tag must be formed to protect the vested interests of all parties.

A single party's contribution taken alone may be included in a protected information unit but it must be protected by the information protection tag agreed to by all the parties to the transaction.

An authorized recipient of an already formed protected information unit can enter it into a new transaction but the preexisting information protection tag must be preserved in the new information protection tag created for the new transaction. The new information protection tag can only be as or more restrictive than the old information protection tag.

### **1.3.2.3 Sequential Steps Towards Establishment of System Operation**

Figure 1.1 illustrates in a simplified form the sequential steps necessary to establish the system, from ground breaking to the transfer of information. Multiple activities (steps) in the same enclosing box can be accomplished independently of one another. This figure is placed here to introduce some of the concepts of the design but a complete understanding of them requires the explanations found throughout the remainder of the paper.

The following pertain to each step:

Step 1: The central (certificating) authority (CA) is established with a private/public key pair. This step is carried out only one time.

Step 2a: Groupings of information usage influences are formulated under the direct or indirect control of the CA. Each entry in a grouping specifies an

information usage influence and how to verify its presence at an information watchdog protected device (IWD).

- Step 2b: IWDs are manufactured. During manufacture the public key of the central authority and the private key of the specific device are securely implanted.
- Step 3a: Information usage influences that are valid at an IWD are made into certificated tokens using the procedures established and directly or indirectly administered by the CA.
- Step 3b: Information usage influences are selected for inclusion in the access control list which is associated with information which is generated within the IWD. The generation of the access control list generally precedes the generation of the information.
- Step 4: An IWD (A) wants to receive information from another IWD (B). IWD A presents its tokens to IWD B. IWD B based on a match of the tokens with the access control list determines if the information can be sent to IWD A. (Each of IWD A's tokens also contains the device ID of IWD A.)
- Step 5: If a successful match is made, the sending device (IWD B) sends the information to the receiving device (IWD A). Prior to transmission, the sending device encrypts the information with the public key of the

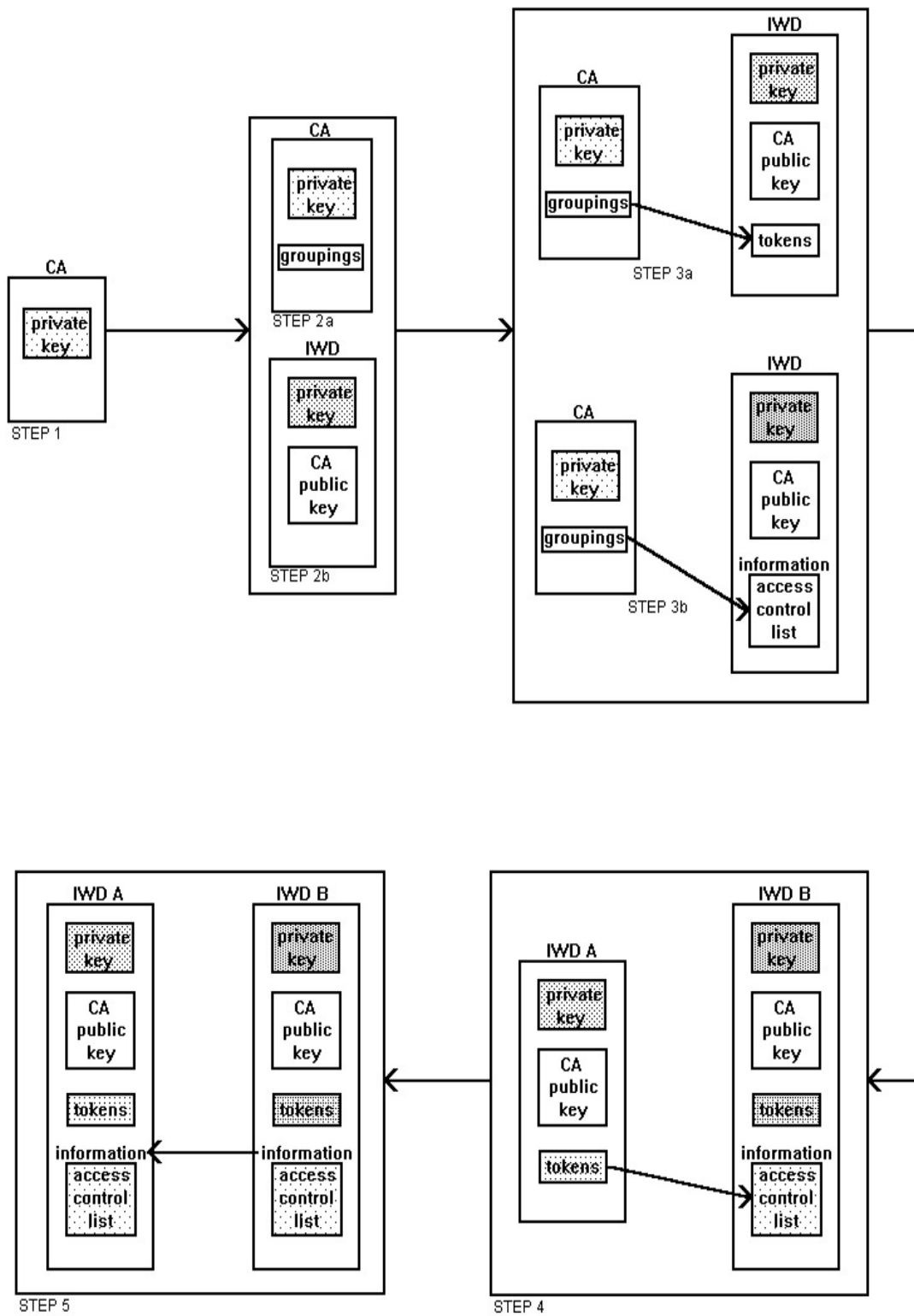


Figure 1.1 Sequential steps to establish system and transfer information

receiving device. The device ID shared by all the tokens, assures that only a device which has an acceptable combination of tokens is able to gain access to the information.

#### 1.4 Background

This paper builds upon the work of others. Chapters 2, 3, and 4 which comprise the body of this paper each deal with a different but related aspect of information protection. The known articles, standards, and previously existing methods which form the foundation for the ideas developed in this paper are given below for each of these chapters.

Chapter 2 describes a method for categorizing the entities that an originator of information can specify as allowed recipients. This leads to the formation of an access control list. The access control scheme developed in this paper builds upon aspects of the Department of Defense's military security policy. Within the military policy, a classification consists of two parts -- a security level and a set of categories. The security level is a hierarchically based classification and is assigned to information based on its sensitivity. A category is an organizational unit to which the information may need to be accessible. There is an implied Boolean AND operation between the security level and the set of categories, and there is an implied OR operation between members of the category set. This paper develops the concept of the information usage influence which generalizes the military policy by allowing each category to have a unique hierarchical (security level) structure and by allowing for the AND operation to be applied to multiple information usage influences to create a description of the state of a device that can access a particular unit of information. The structure for an information usage influence is based on some of the methods used to form tree structures described in CCITT Recommendation X.501, "The Directory - Models" [4], and the

format for an information access control list makes use of the syntax specified in CCITT Recommendation X.208, "Specification of Abstract Syntax Notation One (ASN.1)" [2].

Chapter 3 which deals with communications between devices largely deals with the concepts of public key cryptography as originated and presented by Whitfield Diffie and Martin E. Hellman in their paper "New Directions in Cryptography" [5]. Two advantages of public key cryptography over traditional cryptography are discussed in their paper -- the elimination of the need for the confidential distribution of keys and the ability to apply a digital signature to a digital message. The integrity of distributed keys must also be maintained and Roger M. Needham and Michael D. Schroeder in their paper "Using Encryption for Authentication in Large Networks of Computers" [6] discuss the use of an authentication server, using its private key to sign the public key of a user in its system, as a way of ensuring the integrity of the public key. The terminology used for an authenticating server in CCITT Recommendation X.509, "The Directory - Authentication Framework" [7] is a certification authority. This paper uses the terminology and notation of CCITT X.509 and uses the concept of the certification authority to authenticate public keys as well as validated information usage influences. Certification authorities can be chained and this paper adds structure to this by proposing the need for a middle-tier authority called a validation authority that would perform an established (possibly automated) procedure to authenticate the relationship between an information usage influence and a device ID -- examples of these procedures are given. This satisfies a need similar to that which exists for the assignment of security levels under the military security policy.

Chapter 4 develops the architecture of a compliant device. The internal control of a device is achieved by applying multiprogramming concepts so that the resources of a single device can be shared by information protected by different information access control lists. This view of the operating system as a resource manager is based on the

book Operating Systems [8] by Stuart E. Madnick and John J. Donovan. This multiprogramming approach is made internally secure through the use of a hierarchical ring structure. One of the first implementations of such a structure is described in the paper, "The Structure of the "THE" - Multiprogramming System" [9] by Edsger W. Dijkstra. One of the first systems in which such a structure was implemented in hardware was the Multics system as discussed in the paper, "A Hardware Architecture for Implementing Protection Rings" [10] by Michael D. Schroeder and Jerome H. Saltzer. The ring structure provides an operating mechanism, and a structured design methodology.

The public key of a certification authority, in previous papers, gained its integrity from its highly public status -- an administrator of a computer system could verify the public key by referencing and judging the reliability of numerous sources. This paper describes a device which can not rely on an administrator to perform such a function and so information relating to the certification authorities and the device ID (both private and public components), must be embedded, during the manufacturing process, in the inner ring. The construction of the inner ring and its placement within the device to impede all attempts of physical access are new concerns for the ring structure.

Chapter 5 discusses how this fairly complex system which requires the implementation of a number of interdependent parts can be partially unbundled so that a practical path can exist for its gradual implementation and acceptance in the marketplace. The system developed in these chapters can change the everyday world of information transfer from being a non-trusted environment to being what can be called the Protected Information Environment.



The Appendix discusses an alternate approach to protect information, which depends on highly trusted information systems. A highly trusted system can be used with the Protected Information Environment to allow for a greater number of information security options.

### 1.5 Overview of Threats and Countermeasures

One of the main points developed in this paper is the consideration that must be given to the design of a device in regards to physical security (see Section 4.2) so that it is clear when information is being transferred between devices and thus require the protection mechanisms discussed in Chapter 3, "Communications Between Devices", versus when information is being processed within a device and thus require the protection mechanisms discussed in Chapter 4, "The Information Watchdog". To a large degree, the objectives of an interloper can be directed to information being transferred or processed, and so for each threat, the countermeasures for the threat "Between Devices" and "Within a Device" will be given. Since these protection mechanisms are discussed throughout the paper, in this section a protection mechanism will be described with a brief statement and a reference to a section within the paper. Voydock and Kent in their paper "Security Mechanisms in High-Level Network Protocols" [11], classify the kinds of attacks that can be attempted against a communications channel. The main threat classifications in this section use their terminology. The threats discussed in this section can come from an intentional effort to subvert the system. They can also come from a lack of diligence resulting from the lure of expediency or from a misunderstanding of the restrictions specified in an information access control list. The strong protection measures instituted to counter the intentional effort should benefit the unintentional mishap.

Although the existence of effective countermeasures to possible threats is an important part of this paper, the primary goal of this paper is to discuss an expanded

application of information security. Certain obvious as well as hidden limitations may exist. The obvious ones can be planned for by the information originator. The hidden ones must be found by ethical people and then either corrected or made well known.

- Threat: Release of Message Contents. The confidentiality of the information section of a message must be maintained.

Countermeasures Between Devices: An interloper's attempt to tap a communications channel can be thwarted with encryption techniques. See Section 3.3.1. This paper is not concerned with the details of the encryption algorithms that may be used. It is required that the algorithms be secure against a chosen plaintext attack since public keys will be in the public domain. From the perspective of the information watchdog as a resource manager, communications between devices falls under device management as discussed in Section 4.3.2. Encrypted information can be understood if the decryption key is known. As discussed in the referenced section, private keys and symmetrical keys are only known by the information watchdog so that persons involved with authorized devices can not intercept transferred information.

Countermeasures Within a Device: Data confidentiality can be compromised through external and internal attacks. An external attack consists of physically manipulating a device so that information is exposed. This type of attack is prevented through proper construction techniques. If equipment can not be impervious to alteration then an attempt at alteration should result in the destruction of the equipment. Some construction techniques are given in Section 4.2.1. A related technique must also shield-in electromagnetic radiation. A device may consist of nonvolatile memory or storage. Since the removal of such a subassembly may leave the information intact, information must be stored in encrypted form.

Since a compliant device can fully exist in the private domain of a person, it is not inconceivable that with enough effort at "hacking", the device's bus can be exposed. To this can be connected a non-compliant device so that information processing, on the full stream of incoming information, can proceed without regard to the restrictions specified in the information access control list. Such breakdowns of security must be avoided but as a consolation, as explained in Section 3.4.1, before information can enter a device, the device must be authorized to receive the information. As explained under the threat of spurious association initiation, the identity of a device can not be falsified by physically accessing its inners.

It may be easier for an interloper to steal a device that is already authorized to receive certain types of information. Each validated usage influence is active for a certain period of time, and within that window, intrusion may be successful. Perhaps a method to notify all devices in the system of lost or stolen devices, in a similar vein to that which exists for credit cards, would to a considerable degree amend the problem. Information which requires the active presence of a particular person, as discussed in Section 3.4.7.4, is immune to the stolen device threat unless physical coercion is applied to the authorized person by the interloper.

External controls have also generally included procedural controls. The reliance placed on procedural controls can be lessened with this system since an objective of this system is to keep information within the system as much and as long as possible. The information access control list developed in Chapter 2 gives the originators of information strong specification abilities.

Information can still leave the system via authorized users through paraphrasing. Person to person communication can not be controlled using

technical means, if only due to civil rights issues. However, an established approach is provided as part of the protocol involving the information access control list, for originators to assign openly accessible key words to a unit of information so that various parties, using computer systems, can in a semi-automated mode become informed as to what information is available. See Section 2.5.1.

Internal controls prevent user software from accessing information for which they are not authorized. The information and memory management functions of the information watchdog are primarily concerned with keeping separations between incompatible protected units of information. The rules which govern how information access control lists are interpreted are based on set theory and Boolean algebra and are given in Section 2.1.2. Memory is controlled so that data items can not be indiscriminately mixed -- an application of multiprogramming techniques. See Sections 4.3.1 and 4.3.3.

- Threat: Traffic Analysis. An interloper may try to determine the frequency and length of message communications between parties. From this and possible other knowledge, inferences can be made.

Countermeasures Between Devices: Routing information must be accessible at each relay. The topic of policy routing is briefly brought up in Sections 3.5.3 and 3.5.4, where an originator of information can specify the acceptable communication paths -- those that are deemed more secure or trustworthy. The Appendix describes an architecture which can promote trustworthiness within a system in which the originator does not deem it worthy to fully specify which devices can receive the information.

Countermeasures Within a Device: The sending or receiving of a message is accomplished at a device within the information watchdog. Any nonconfidential

fields of messages existing within a device can be made available to all usage states of the device at the discretion of the device's administrator. Otherwise, access to header information is not openly available.

- Threat: Message Stream Modification. An interloper may try to alter a message in order to influence the actions of the message recipient. Related to this an originator of information may try to repudiate his originator status in order to become absolved of an obligation or responsibility.

Countermeasures Between Devices: A digital signature using a hash function and a private key can prevent the alteration of a message. See Section 3.3.2.

Countermeasures Within a Device: The digital signature can apply here as well except that the public/private key pair has been thought of as belonging to the device in total. Possibly some complications may arise if a key pair is assigned to each usage state. Instead, for intra-device integrity, at a level of the operating system higher than the information watchdog, a user-indicating origination/modification code can be assigned to processed information.

- Threat: Spurious Association Initiation. An interloper may try to obtain information, or more generally form a communications association, by representing himself with a false information usage state.

Countermeasures Between Devices: Each usage influence which is to be included within a device's credentials must be validated by an independent trustworthy procedure which can be manual or automated. A token is then created containing the usage influence and the associated device ID or personal biometric identifiers. The token is signed by the validation authority in order to maintain the integrity of the token. The public key of a device is also validated in a similar manner. Via the device ID, the public key of a device is related to the validated usage influences of a device. The "channel" created by a public key

is thus authenticated to senders of information. See Section 3.4. As explained in the referenced section, the ultimate integrity of the overall system rests with the confidentiality of the private key of the certification authority. If this key is compromised, false authenticated public keys and usage influences can be issued. Since the public key corresponding to the certification authority's private key is embedded in each device during manufacturing, the ability to decommission a key and institute a new key pair must be incorporated into the device during manufacturing. This can be accomplished by embedding multiple certifying public keys within each device so that a switch to a new key can be made. Each certifying private key should be administered separately to diminish the possibility that more than one key is compromised as the result of a single breach in security.

Just as compliant devices must be made tamper proof so too must the procedures used by certification authorities and validation authorities. Some of what they do may be largely based on human procedure. For instance, some information usage influence validations may require that an audit be performed. Each validated usage influence assigned in this manner is dependent on the ethical behavior of human beings. Internal controls should be instituted to shape human behavior in a vein similar to that which exists within a business for the protection of assets. If a breach in security occurs at one of these authorities, a means would need to exist to detect the breach.

Countermeasures Within a Device: Protected information is sent to an information watchdog at a device. It is the information watchdog's responsibility to allow only authorized information usage states at a device to access the information. The processor management function of the information watchdog

accomplishes this by gathering the usage influences of a usage state and by verifying that they are all currently validated. See Section 4.3.4.

## **CHAPTER 2**

### **THE INFORMATION PROTECTION TAG**

#### 2.1 Introduction

In Section 1.3.1 it was stated:

In a limited environment, the designations in an access control list can be simple. For instance, the military has unclassified, confidential, secret, and top secret; a commercial computer may have work groups and user IDs. The relationships of entities in the everyday world are very complex and so these relationships need to be understood in order to form precise (as well as concise) access control lists.

This chapter will develop a fundamental way of classifying information usage and will incorporate this into an approach for specifying the allowed usage of information.

##### 2.1.1 Information Usage States and Influences

A party in possession of information may want to restrict the distribution of the information to include only certain parties. In order to distinguish one party from another and to allow for more awareness concerning the inclusion of designations in access control lists, parties will be called and thought of as information usage states. A usage state is a combination of information usage influences. A usage influence can be widely applicable in that it can be used in conjunction with other usage influences to define many usage states. A usage influence is the most basic way of distinguishing something that can have an influence on the way information is used. Usage influences



with similar qualities are assigned to the same grouping of usage influences. A usage influence is designated by a grouping, and by an instance within the grouping. (As will be explained later after the Information Distribution Directory is introduced, the instance within a grouping can consist of entries along a directed path of a hierarchical structure.) Examples of groupings include the physical locations of devices, the computing power of devices, the software applications that run on devices, and the organizational responsibilities of device users. Each instance within a grouping must be able to be uniquely distinguished. As an example of instances within a grouping, an "organizational responsibilities of device users" grouping may have instances of salesperson, and secretary. Since groupings are unique and instances within groupings are unique, usage influences can be uniquely specified. In set notation, a grouping of influences is a set consisting of information usage influences, and

$$UsageUniverse = \cup_{i=1}^n Grouping_i, \text{ where}$$

$$Grouping_i \cap Grouping_j = null, \forall i \neq j$$

### 2.1.1.1 Usage Influences Clarify the "Need to Know" Concept

A common basis for controlling access to information is the need to know concept. This concept can be analyzed. One assertion that the assignment of an access designation based on this concept makes is that there is some party performing an operation and that the operation requires the information. By allowing that party to access the information, it is also being asserted that it is acceptable for the information to be used in a certain way, as determined by the operation.

The concept of the information usage influence attempts to get at the essence of the concern with restricting information access -- it tries to restrict the use of information. Whereas a need to know restriction implies a use of information, a usage influence specifies the allowed usage of information. More specifically, the usage of information can not be directly controlled, but rather the allowed influences which

determine how information is used can be specified. Candidates for (groupings of) information usage influences are given later. The common information restriction based on trustworthiness is an aspect of some of them since trustworthiness can influence the usage of information.

#### **2.1.1.2 Usage Influences Reflect and Shape the Real World**

The concept of the usage influence is intended to reflect the real world but in order for it to always be applicable, the real world may in some instances need to be fashioned to fit the concept of the usage influence. For instance, a computer program may perform two different functions, i.e., billing and market analysis. For the creator of an access control list to be able to specify that the associated information is only to be distributed to billing programs, the market analysis function must be separated from the billing function in such a way that when the information is being processed, only the billing function (usage influence) is able to access the information.

#### **2.1.1.3 Usage States Describe, They Do Not Identify**

This classification system is not intended to uniquely identify recipients (realized usage states). For instance, it may seem that the usage influence of a particular work related role may have many potential recipients, whereas the usage influence of a particular person narrows the field down uniquely, after all each person is unique. But just as many people can engage in a line of work, a single person can run many applications, use many computers, or work at many locations. Each information watchdog is assigned an ID, and although this uniquely identifies a device, the same reasoning shows that it also does not uniquely identify a recipient. In some instances, a usage state can be so limited or specific that it is realized by only a single occurrence, thus seeming to uniquely identify that recipient. But the identification is not complete because at another moment, another realization of the same usage state may come about.

Therefore, when transferring information, the recipient should be identified using the identification approach devised for the channel, i.e., telephone numbers, presentation service access points (PSAPs). Also, just as the expression of a thought is limited to the available words, a recipient's usage of information can only be expressed with the available (at the time) usage influences -- a usage state which consists of usage influences can only describe, not identify.

#### **2.1.1.4 Usage States Exist in a Multi-dimensional Space**

Since information usage influences from the same grouping are mutually exclusive, an information usage state can not contain more than one usage influence from the same grouping. A grouping of influences can be considered a dimension in informational usage space and a usage state exists in this multidimensional space by being defined once for each dimension. If there are  $n_1$  usage influences in grouping 1,  $n_2$  usage influences in grouping 2, and  $n_3$  usage influences in grouping 3, for a total of  $n_1+n_2+n_3$  usage influences (where each  $n$  includes the null member) then the number of possible usage states is  $n_1n_2n_3$ .

#### 2.1.2 The Information Access Control List

An Information Access Control List (IACL) is an unordered list of usage states. A unit of protected information has a single IACL associated with it. A device has device credentials, the equivalent of an IACL, associated with it. The information watchdog performs four operations which involve the contents of IACLs and device credentials. These operations determine if a PIU can be transferred to another specific device, if a PIU can be read accessed by a specific usage state at a device, and if a PIU can be write accessed by a data structure protected by a specific IACL. An operation is also needed to combine IACLs associated with units of protected information which are being aggregated. These operations are discussed below:

### 2.1.2.1 Permission to Transfer (Read) Information

In order for protected information to be sent to another device, the sending device must do a comparison between the IACL associated with the protected information and the device credentials associated with the receiving device. In set notation, for a transfer to be permitted:

$$IACL \cap Device\ Credentials \neq \emptyset,$$

that is at least a single usage state allowed access to the information must be present in the device. For a usage state associated with information (*I-US*) to match a usage state associated with a device (*D-US*):

$$I-US \subseteq D-US,$$

that is all the usage influences in a usage state associated with information must be members of a usage state associated with a device. Usage influences generally require that their existence at a device be independently validated before they can be associated with the device. In order to read information a two step process occurs. First the information watchdog must gain access to the information based on a device's credentials. Then at the device, a recipient can read the information based on its usage state.

### 2.1.2.2 Permission to Write Information

For the writing of protected information to be permitted:

$$IACL_{write\ access} \subseteq IACL_{read\ access},$$

that is every usage state assigned to the write file must be present in the read file. For a usage state associated with a write access file (*W-US*) to match a usage state associated with a read access file (*R-US*):

$$R-US \subseteq W-US,$$

that is all the usage influences in a usage state associated with a read file must be members of a usage state associated with the write file.

A difference between read access device credentials and a write access IACL is that the device credentials can contain usage states which are not present in the IACL associated with the information to be read, whereas all the usage states within the write access IACL must be present in the IACL associated with the information to be read.

### 2.1.2.3 Boolean Algebra

A particularly meaningful way of representing an IACL is with Boolean algebra. The AND operation applied to usage influences creates an information usage state and the OR operation applied to usage states creates an IACL. Let each letter of the alphabet represent a grouping of usage influences,  $A, B, C, \dots$  so that  $A_1, B_1, C_1, \dots$  are information usage influences within their respective groupings. Therefore, applying the AND and OR operations,  $C_{14}P_{57}A_3G_{26}+M_2B_{19}+H_7C_{14}P_{57}$  is an IACL consisting of three usage states. Each usage influence is a variable, each usage state is a product of variables, and each IACL is a sum of product terms. Each usage influence, as explained later, is assigned a numerical value, but this value is used for representational and ordering purposes and so the summation and product operations should not actually be performed on these values. Instead, the presence of a usage influence in a device's credentials indicates the TRUE condition, and its absence indicates the FALSE condition. If the evaluation of an IACL Boolean expression results in the TRUE condition, then the device can access the associated information.

The perspective of Boolean algebra is of great practical help when IACLs are combined as a result of the aggregation of protected information units. The combined IACL must maintain the access requirements of all the individual IACLs and thus be as or more restrictive than each individual IACL. This can be partially accomplished by applying the AND operation to the individual IACLs. For instance, if:

$$\begin{aligned}
IACL_1 &= A_1C_7+G_6, \text{ and} \\
IACL_2 &= B_2G_8, \text{ then} \\
IACL_{product} &= (A_1C_7+G_6)(B_2G_8) \\
&= A_1C_7B_2G_8+G_6B_2G_8
\end{aligned}$$

Since two usage influences from the same usage grouping are mutually exclusive, the last term is not allowed. For instance  $G_6$  could be Location=USA and  $G_8$  could be Location=France. Therefore,  $IACL_{combined} = A_1C_7B_2G_8$ .

Algebraic simplification of a combined IACL should be done within an information watchdog in order to reduce the IACL to the minimum number of terms. The rich body of Boolean operations, theorems, and reduction techniques can be used.

## 2.2 A Selection of Groupings of Usage Influences

A usage grouping is needed for each type of influence which can affect how information is used. Usage determines the value of information for both proprietary and privacy concerns. The proprietary concern usually puts more importance on controlling the quantitative usage of information rather than the qualitative, although the qualitative aspect may be important when a proprietor wants to be remunerated with what a particular usage market segment is willing to bear. The privacy concern puts more importance on the qualitative. The qualitative usage of information can not be directly controlled since that would require the invasion of inner sanctums -- the daily functioning of an office or even the functioning of the human mind. Where society deems it important enough though, the law can intervene. For instance, a hiring decision, based on certain information, can not be directly affected by this technologic solution but it can be directly influenced by anti-discrimination laws. In terms of a technologic solution, the influences on information usage can be determined, and information usage can be indirectly controlled by selectively restricting the information's accessibility to these influences.

Protected information, both proprietary and private, has the starting point of not being accessible to any influence. Upon this, accessibility to influences is selectively permitted by placing usage influences, each picked from a different grouping, into usage states. Some groupings of usage influences and their influences on information usage are given:

- Line of Business -- This influences how information may be turned into a product or service. The media and direct marketing data base (junk mail) businesses may be of general concern. This usage grouping can also help prevent conflict of interest within a company. Within the mergers and acquisitions department of an investment bank, the acquisition price of a client firm should create different motivations than the same information in the bank's portfolio management department.
- Processing Function -- This grouping, which usually involves software applications, influences how information is analyzed and acted upon.
- Device Type -- The power and specialized features of a processing device such as a computer can influence how efficiently and effectively information is processed. In terms of proprietary software (a major form of proprietary information), if its installation on a personal computer is one unit of usage, then its installation on a mainframe is many units of usage. The device type can determine the type of information output which can occur.
- Work Related Role -- This influences how information is interpreted, including the application of training, experience, and professional ethics.
- Person -- Personal outlook and personal relationships can influence the way information is used. A person's trustworthiness is of particular importance.
- Administration -- This includes both the Organizational Unit and Organizational Position groupings discussed later. This involves the control mechanism to

allocate, coordinate, and protect resources. An administrative unit or position is included in a usage state because particular trust is placed in the control mechanism that it will protect the information. This grouping is an adjunct to the information watchdog. Although procedural threats to information protection are minimized by the information watchdog, they can still exist. A trusted administrative unit or position can provide further protection. The word trust is significant here since an Administration usage influence does not specify how information is to be used other than that proper intentions be applied. A formal set of procedures can be devised for the audit and attestation of the robustness of an organization's information processing privacy protections. Lessons learned with audits conducted in regards to a public corporation's financial statements, may apply. Appendix A discusses the audit need in conjunction with principles which can be followed to create secure processing within an organization.

- Device ID -- This identifies a piece of hardware via the information watchdog's identifying code. A device like an administrative unit or position is a control mechanism to allocate, coordinate, and protect resources. Although a device must be designed so that it is protected from the non-trusted environment, compromise is a possibility. A device ID is included in a usage state because particular trust is placed in that device.
- Time -- Information may be valid for a limited time. Information may be needed now to accomplish a desired outcome but may be counter productive or may cause confusion over a future outcome.
- Location -- The physical placement of information influences the type and degree of observation which can be made of the use of information. Greater observation affords a greater ability to control. For instance, if a company's trade secrets can only be accessed within the physical facilities of the company then observability



of use is much greater than if the information is accessed away from the company's facilities. Location also determines legal jurisdiction. This influences which laws apply to the use of information. This can be very broad and can range from the illegality of information based on political or moral grounds, to the rights bestowed on information as property in the marketplace. The police powers which back up these laws supply another level of information protection.

### 2.3 The Data Base of Usage Influences

Given that usage influences associated with information must match usage influences associated with a device before the device can receive the information, the possible usage influences that can be placed within usage states must be decided upon beforehand and made available to all parties formulating IACLs and device credentials. This requires some generally accessible data base of usage influences. The scope and accessibility of such a data base must correspond to the scope of those who will be involved with the transfer of information. The most inclusive data base would contain information usage influences applicable to the world-wide usage of information and it would need to be accessible on a global scale. The central certificating authority exercises oversight control over the formation of information usage influences so that there is no redundancy. As explained in Section 2.4.3, administrative control can be decentralized in conjunction with entries on a specified tree structure in the data base. Over time the data base can grow, as new useful usage influences are identified.

The data base service offered by the Directory as described in the X.500 [1] series of CCITT Recommendations offers general concepts, terminology, as well as specific services, which can be borrowed in part to implement the data base of usage influences. X.500 calls its data base the Directory Information Base. To distinguish this derivation of the Directory from actual implementations of it, the data base for

information protection will be called the Information Distribution Directory (IDD). The IDD answers the need described in Section 1.3.1:

In a limited environment, it can be relatively easy for a person generating information to find out the designations, in terms of spelling, syntax and semantics, which he wants to include in the access control list associated with the information. The everyday world requires a universally accessible data base of entity designations. The concepts described in CCITT X.500 [1] can be applied to this need.

The Directory as described in the X.500 series consists of a hierarchical tree structure. A tree is a set of points called vertices, and a set of directed lines, called arcs, where each arc leads from one vertex to another. At each vertex is an entry. An entry consists of one or more attributes and an attribute consists of its type and one or more values. The attribute types and the syntax for the attribute values are defined for an object class. An entry is formed by assigning syntactically correct values to the attribute types of an object class. The IDD uses the general concept and terminology of object class, entry, and attribute.

The tree structure described in X.500 can also be used for the IDD. Each usage grouping is independent of the other usage groupings and so each usage grouping has its own tree -- within a grouping the usage influences can be related hierarchically. A usage influence, in such a case, consists of an ordered list of entries found consecutively along a directed path from a root entry to another entry at a lower position on the path. A given tree structure is allowed to have more than one root.

The fact that a usage grouping can usually be structured in alternative ways, where one approach is as acceptable as another, needs to be resolved. For instance, a location could be specified hierarchically using political divisions such as nation, state, county, etc. or could be specified continuously using two dimensional ranges of latitude and longitude.

## 2.4 Attribute Categories of the Information Distribution Directory

There are four main categories of attributes for the IDD:

- Syntactical
- Naming
- Informational
- Controlling

### 2.4.1 Syntactical Attribute Category

The syntactical category has one attribute which identifies the object class to which an entry belongs. This attribute is a code, unique within the IDD, which can be used to reference, in a data base of object classes, the fields and syntax of each field, and general information as to why this object class is needed. Figure 2.1 will be used in this section to illustrate certain ideas. The object class of each entry is specified here with a descriptive term, i.e., Company or Division, (normally a code is used), and each instance of an entry is specified with an identifying code.

An object class should be assigned to an entry based on the entry's need for certain attributes, but otherwise there is nothing inherent about the structure of a grouping which prohibits a vertex from being associated with any object class. For instance, one company may be organized as is Company 1 in Figure 2.1, whereas another company, such as Company 2 in Figure 2.1, may consist of a single level of sub-units (not shown). The attributes to be associated with Company 2's sub-units may

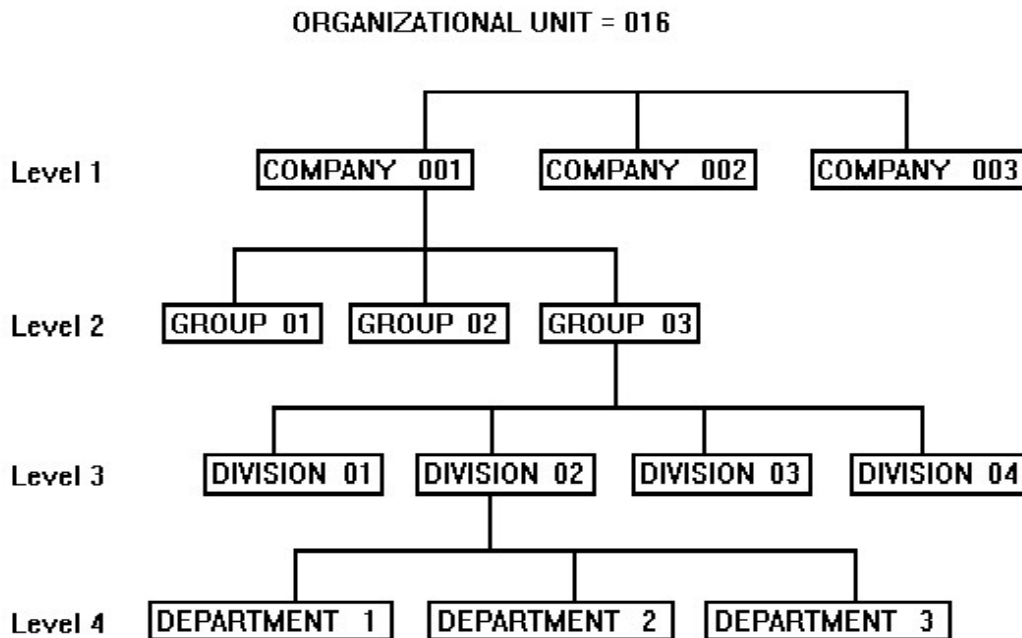


Figure 2.1 The Organizational Unit hierarchical usage grouping

be specific to those sub-units and so require their own object class. Even entries with the same parent can have different object classes. For instance, for a grouping of Location based on political divisions, the entry of the U.S. doesn't just have subordinates of states but also of protectorates, territories, and possessions -- each one may need its own object class.

#### 2.4.2 Naming Attribute Category

The naming attribute category depends on if the usage influences are continuous or discontinuous. Discontinuous usage influences require a hierarchical structure whereas continuous usage influences can use a flat or hierarchical structure. Figure 2.1 is an example of a discontinuous usage grouping. Group 1 and Group 2 are both members of Company 1 but the entries they "group" are more related within a group than

between groups. Other types of usage influences are continuous in relation to one another. An example is the specification of the power of a computing device with a standard measure. The naming attribute category will be discussed first for the discontinuous case.

#### **2.4.2.1 Discontinuous Groupings**

The naming attribute category for the discontinuous case consists of two attributes. One attribute gives the size of the field containing the entry's identifying code and the other attribute gives the code. Normally the size of a field is specified by the syntax of the object class but the size of an entry's identifying code varies based on the number of entries that are possible under a parent. All entries with the same immediate parent entry must have the same field size for the code. The code only uniquely identifies an entry in relation to the other entries with the same parent. For instance, level 1 in Figure 2.1 has an identifying code size of 3 octets.

As expressed earlier, a usage influence is designated by a grouping, and by an instance within a grouping. Each grouping, such as the Organizational Unit of Figure 2.1, is given an identifying code. This code is not included in an entry but exists in a data item that is applicable to the entire tree structure. An instance within a structured grouping is given a code which is formed by concatenating the identifying codes assigned to each entry along a directed path -- this will be called a concatenated code. Therefore, a usage influence is identified by:

$$\text{Usage Grouping Code} = \text{Concatenated Code}$$

For instance, in Figure 2.1, the usage influence which includes Department 1, would have a code 016=00103021. Just as a usage state exists within a multidimensional space where each dimension is a grouping of usage influences, each dimension has an axis along which usage influences are indicated by discrete points (for continuous groupings the values along the axis are continuous).

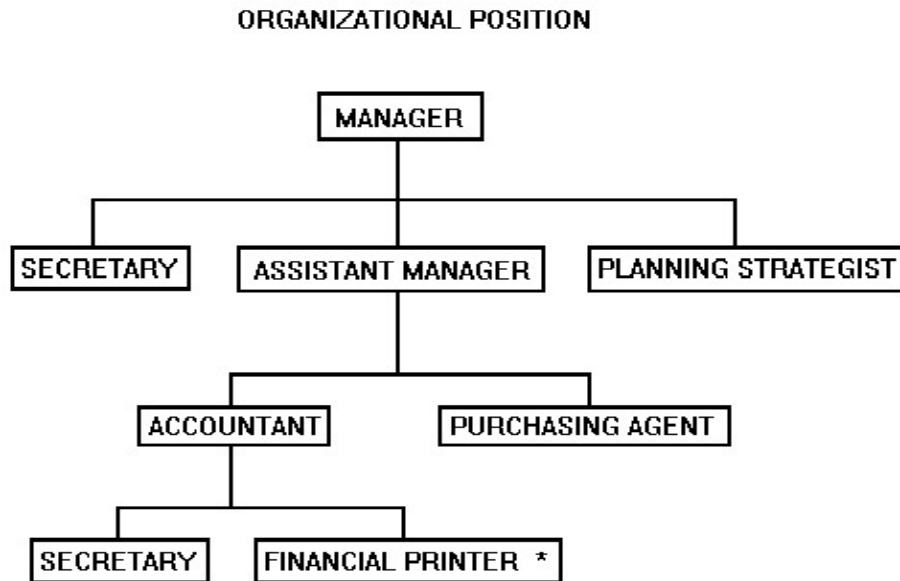
By hierarchically ordering entries in a meaningful way, usage influences can be included in meaningful ranges. This allows for conciseness when usage states are selected for inclusion in IACLs. For instance, referring to Figure 2.1, if each department within Division 2 is to be allowed to receive a particular unit of protected information then three different usage states, one for each department, would need to be included in the IACL. But by specifying an implied range of usage influences as with 016=0010302, all of the departments in Division 2 are included. The term aggregated usage influence will apply to all ordered entries found along a directed path which do not end with an entry at a leaf vertex.

#### **2.4.2.2 Validation of Hierarchical Usage Influences**

At a device, a validated usage influence is formed by validating all consecutive entries between a root entry and an ending entry which may or may not be a leaf entry. A validated usage influence (which is associated with a device) is successfully matched with all aggregated usage influences (which are associated with information) which end with the same or with a preceding entry along the path of the validated usage influence. For instance, in Figure 2-1, a validated usage influence ending with the Division 02 entry can successfully match an aggregated usage influence ending with Division 02, Group 03, or Company 001, but can not match a usage influence ending with Department 2. This is because children entries can be considered a partitioning of the information usage aspects of a parent. Therefore a child is a more narrowly focused aspect of a parent. If information can be received by a parent then this implies that any of its children can also receive the information; whereas the reverse is not true. Therefore a device validated at a certain level of a tree can receive all information with access restricted to entries at the same level or above, along the same branch.

### 2.4.2.3 Forming Hierarchical Groupings

The thought process that is involved with selecting usage groupings and with the structuring of entries to form usage influences will be shown with an example. Such work related terms as manager, secretary, accountant, etc. in the information usage universe actually can signify two separate usage groups -- Organizational Position and Work Related Role. The Organizational Position grouping represents the hierarchical reporting structure of job positions in a specific company -- the placement of an entry in the IDD is dependent on the information flow. On the other hand, the Work Related Role grouping represents the structure which indicates the nature of the duties performed by a job position -- the placement of an entry in the IDD is dependent on the type of information interpretation that is done. In a sense, an Organizational Position is filled by a Work Related Role.



**\* Positions can extend beyond bounds of formal organization.**

Figure 2.2 The Organizational Position of usage influences. For illustrative purposes, each entry is identified with a descriptive term instead of a code.

Figure 2.2 and Figure 2.3 will be used in this section to illustrate certain ideas. Their entries omit the object class as was shown in Figure 2.1. Figure 2.2 shows an abbreviated structure of the Organizational Position grouping and Figure 2.3 shows an abbreviated structure of the Work Related Role grouping. The Organizational Position grouping is really a continuation of the Organizational Unit grouping of Figure 2.1, and fits in where position titles are more appropriate to indicate the hierarchical structure than unit titles. The structure of the Organizational Position grouping is determined for each company by its organizational structure, whereas the structure of the Work Related Role grouping is applicable across all organizations.

The Organizational Position and Work Related Role groupings can be used to specify different allowed usages of information. If information is to be accessed only by people who practice a certain categorization of work, such as all accountants, then Work Related Role is relevant, but if information is to be accessed by a group of positions arranged to accomplish a task, such as an accountant, secretary, and financial printer, then Organizational Position is relevant. To say this another way, just as many departments and divisions need to access information protected by a usage influence which ends with a group (see Figure 2.1), there may be many helping positions which need to access information protected by a usage influence which ends with an accountant (see Figure 2.2). On the other hand, information may need to be accessed by accountants (or hierarchically following accounting specializations) as a category, without this right being given to their subordinate staff (see Figure 2.3).

Just as work related terms can be viewed from two different perspectives, the usage influences in the Organizational Unit grouping, as shown in Figure 2.1, can be viewed from another perspective. In Figure 2.1, the structure is directly concerned with the marshalling of resources into divisions rather than with the products or services that are the business of the division. Another usage grouping can be Line of Business, which



## WORK RELATED ROLE

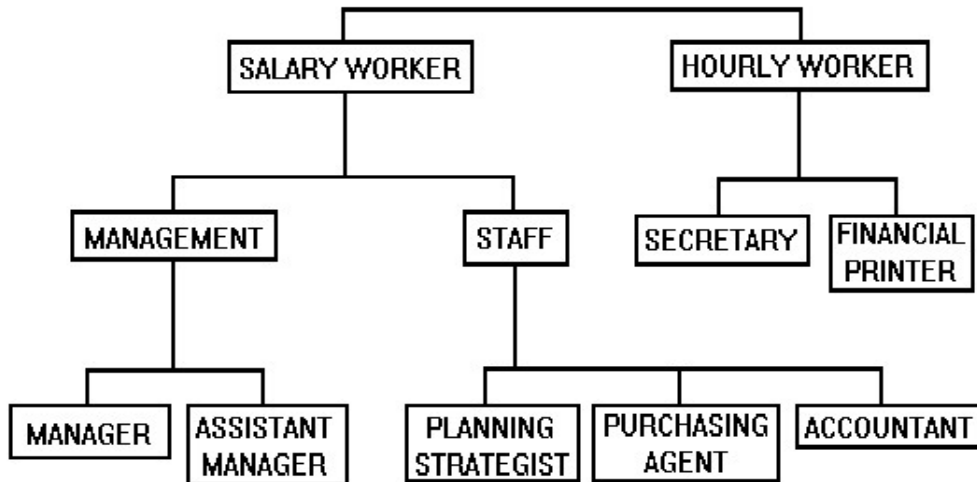


Figure 2.3 The Work Related Role grouping of usage influences. For illustrative purposes, each entry is identified with a descriptive term instead of a code.

is structured in some way based on products and services. For a company to receive information which is protected by an applicable Line of Business usage influence, its organizational structure must be factored at the division, department, or some other level so that the resources of that unit which are involved with information processing, are dedicated (in some reasonable way) to that line of business.

A guideline for the formation of usage groupings is that usage influences selected from two or more groupings should never be mutually exclusive. The usage state formed by these usage influences may not be presently realized but it should not be impossible for it to occur. An example can make use of the Organizational Unit and Line of Business usage groupings. The usage state Line of Business=Bolt Manufacturer,

Organizational Unit=Group ABC within Company XYZ may not be realized since Group ABC only manufactures nuts, but it is not impossible that Company XYZ will reassign the resources of Group ABC in order for it to manufacture bolts.

#### **2.4.2.4 Continuous Groupings**

The naming attribute category will now be discussed for usage influences that are continuous. The continuous nature of usage influences allows for any range to be meaningful. Therefore, a usage influence from a continuous grouping can be identified by:

Usage Grouping Code=Starting Parameter-Ending Parameter

The parameter, such as the standard measure of the power of a computing device, may need to be transformed so that it can be a hexadecimal number that can be contained within a reasonable number of octets. This transformation is made known in the grouping's information section. As discussed later under the control attribute category, there may still be a need to classify ranges of a continuous influence and have them represented by entries. These entries can be arranged in a flat or hierarchical structure. A hierarchical nature is inherent within a continuous grouping though. For instance, the computing power of 10 to 15 MIPS is contained within the computing power of 5 to 20 MIPS. For continuous groupings, the naming attribute category has three attributes. One for the size of the parameter fields, one for the starting parameter value, and one for the ending parameter value. It is also possible that a usage influence will be continuous in two, three or some other multidimensional space. For instance, a location can be specified with latitude and longitude.

#### 2.4.2.5 Aggregated Usage States

Since a usage state exists at a single point in usage space, a new term is needed to indicate an aggregation of usage states formed with aggregated usage influences -- this will be called an aggregated usage state. An aggregated usage state can also be formed by setting a grouping code equal to more than one concatenated code. For instance, the aggregated usage state 016=00103,002 specifies the usage influences pertaining to all the organizational units under Group 3 of Company 1 and all the organizational units under Company 2. An aggregated usage state is like an IACL in that it consists of individual usage states -- the notation allows for conciseness but does not create a new type of usage state. Since, in a sense, an aggregated usage state can consist of a single usage state as well as many usage states, it is simpler to think of an IACL as consisting of an unordered list of aggregated usage states.

Aggregated usage states can be expressed in Boolean notation by applying the OR operation to usage influences within the same grouping. For instance, using the notation of Section 2.1, the following aggregated usage influences and aggregated usage states make up an IACL:

$$\textit{Usage Influence} = B_1$$

$$\textit{Aggregated Usage Influence} = A_1+A_4+A_9$$

$$\textit{Aggregated Usage Influence} = C_1+C_2$$

$$\textit{Aggregated Usage Influence} = E_3+E_{12}$$

$$\textit{Aggregated Usage State} = (A_1+A_4+A_9)B_1$$

$$\textit{Aggregated Usage State} = (C_1+C_2)(E_3+E_{12})$$

$$\textit{IACL} = (A_1+A_4+A_9)B_1 + (C_1+C_2)(E_3+E_{12})$$

The above example is simplified since each usage influence is explicitly stated. For hierarchical groupings, the concatenated code notation allows for Boolean type operations to be performed by an information watchdog, without it knowing the exact

structure of the code. For instance, the summation of two concatenated codes in the same usage grouping, 6135 + 613 results in 613. The product of these codes, (6135)(613) results in 6135. The 6135 is an extension of the 613 and so is included in the 613. That is if  $Y=Y_1+Y_2+Y_3$  then  $Y_1+Y=Y$ , and  $Y_1Y=Y_1+Y_1Y_2+Y_1Y_3 = Y_1(1+Y_2+Y_3) = Y_1$ .

For continuous groupings, the OR operation is performed by the union of sets, and the AND operation is performed by the intersection of sets. For instance, the summation of two ranges in the same usage grouping, (15 to 6B) + (52 to 70) results in 15 to 70. The product of these ranges (15 to 6B)(52 to 70) results in 52 to 6B. This can also be related to Boolean operations by representing a range with consecutive Boolean variables. Let  $Range_A = X_1 + X_2 + X_3 + X_4$  and  $Range_B = X_3 + X_4 + X_5 + X_6$ . Then  $Range_A + Range_B = X_1 + X_2 + X_3 + X_4 + X_5 + X_6$ , which is the union of the two sets.  $(Range_A)(Range_B) = X_1X_3 + X_1X_4 + X_1X_5 + X_1X_6 + X_2X_3 + X_2X_4 + X_2X_5 + X_2X_6 + X_3 + X_3X_4 + X_3X_5 + X_3X_6 + X_3X_4 + X_4 + X_4X_5 + X_4X_6 = X_3 + X_4 + X_1X_5 + X_1X_6 + X_2X_5 + X_2X_6$ . But as explained in Section 2.1, two usage influences from the same usage grouping are mutually exclusive, so the last four terms are not allowed. Therefore the product is  $X_3 + X_4$ , which is the intersection of the two sets.

#### 2.4.2.6 Application of Hierarchical Grouping to U.S. Military Classification System

A well known classification system is that used by the U.S. military. This classification system is hierarchical, similar to the hierarchical structures already shown, but is a special case since each level has only a single entry. Assigning the code 1776 to the MILITARY CLASSIFICATION usage grouping, the following diagrams its hierarchical structure and lists the code for the aggregated usage influence at each entry:

UNCLASSIFIED	1776=1
↓	
CONFIDENTIAL	1776=11
↓	
SECRET	1776=111
↓	
TOP SECRET	1776=1111

Confidential information when aggregated with secret information should result in secret information. Using the technique discussed in Section 2.4.2.5:

$$(IACL1)(IACL2) = \textit{Combined IACL}$$

$$(1776=11)(1776=111) = (1776=111)$$

A validated secret usage influence should be able to receive information labeled as confidential. As explained in Section 2.4.2.2, since secret is a child of confidential as is represented by their code designations, a PIU labeled as confidential can be transferred to a device labeled as secret, the PIU can be accessed by a usage state labeled as secret, and the protected information can be written to a data structure labeled as secret.

#### **2.4.2.7 Multiplication of Sets of Usage Influences Forms Set of Available Usage States**

A tree, for purposes of forming individual information usage influences, can be disassembled into a set of branches, which consist of an ordered set of entries from root to leaf. Since each branch ends with a unique leaf, each branch can be represented by its leaf entry. The set of usage influences for a continuous grouping is theoretically infinite but due to limited word length is finite. If within each set of usage influences is included the null member then the set of all available information usage states is the product of the set of usage influences for each grouping, where the order of usage influences within the result is not important.

### 2.4.3 Informational Attribute Category

There can be a large number of informational attributes for each object class. Informational attributes are needed for a number of reasons. An identifying code (a naming attribute) is used to specify an entry but human intelligible information is needed so that entries can be meaningfully selected. For instance, a person may be assigned a Person ID code but in order for someone to associate the ID code with a person, informational attributes are needed such as the name and address of a person. Therefore, various descriptive informational attributes may be needed to identify an entry. Also validation (as discussed in Section 3.4) is formulated for and applied to each entry in a usage influence. The validation technique for each entry can be indicated in an informational attribute.

Some type of administrative function is needed to determine the structure of a grouping. The administration may be carried out on a centralized or decentralized basis. With a centralized basis, all decisions are made within a single administrative body for the entire grouping. With a decentralized basis, each entry can be represented by an administrative body for decisions regarding the formation of subordinate entries. Information concerning these administrative bodies, such as name, address, and telephone number, can be included as informational attributes within each entry. The values in the naming attributes go into the IACL as usage influences, but the values in the informational attributes stay within the IDD, although they may help with the selection of usage influences.

### 2.4.4 Controlling Attribute Category

The control over how information is used is mainly accomplished by only permitting the distribution of the information to recipients which possess selected usage states. Since particular usage states should use information in particular limited ways, the concern over information usage is largely settled. However, there are certain

controls that can be administered at the recipient's device. For instance, information protected by a usage influence from the Person grouping should be able to be received by a device which is associated with the person identified in the usage influence. But a method should also be available so that the requirement can be made that in order for the information to be processed, the person must indicate his or her presence at the device. After each usage influence, these control attributes and their values can be specified. Generally there will be few of these control attributes, since most control can be accomplished by specifying the allowed distribution. For instance, a software program in the Processing Function usage grouping could offer control attributes which would allow the information originator to enable or disable particular program options at the recipient's device. But this can also be accomplished by factoring the program into separate modules as far as usage influences are concerned. This has the conceptual advantage that factored usage influences can form narrowly focused usage states.

#### **2.4.4.1 Default Controls in the IDD**

Control attributes can be specified for each object class and default values for them can be specified in each entry in the IDD. For hierarchical groupings, the control attributes in the higher level entries should be relatively more general so that they can apply to lower level entries. At the lower level entries, though, where the usage influence is more focused, the control attributes can be more specific, until they may be only applicable to a usage influence ending with a certain leaf entry. A validated usage influence at a device, must have a copy of all the control attributes in the IDD entries along its directed path so that it can have the default values if an IACL has not specified them.

### 2.4.4.2 Device Type Grouping Controls

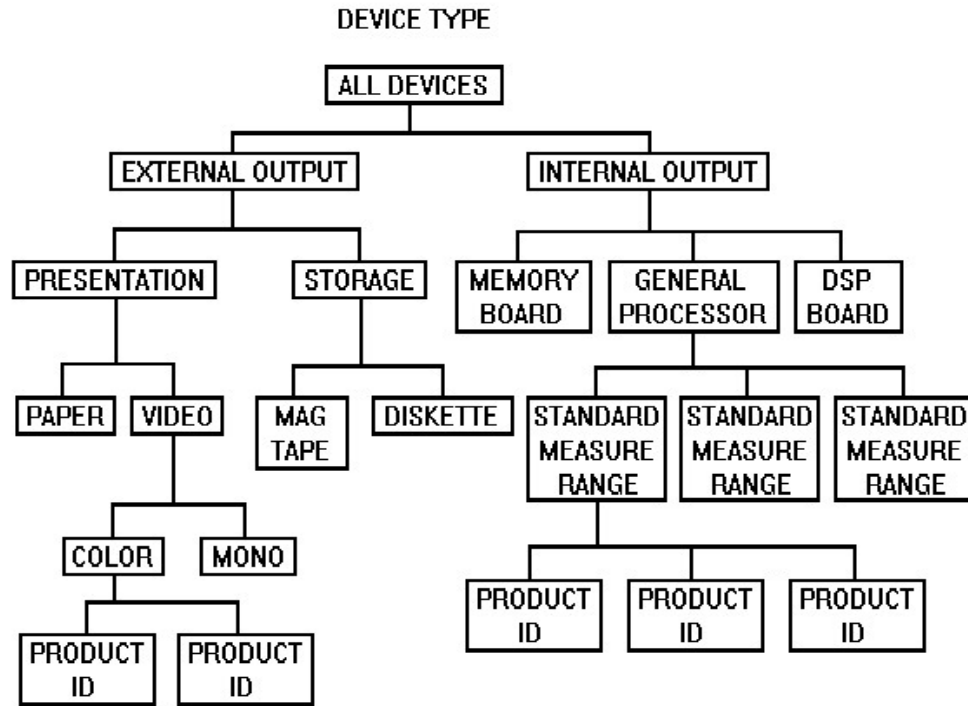


Figure 2.4 The Device Type grouping of usage characteristics

The control attributes for the Device Type grouping primarily involve the output of information and are of great importance since after information leaves the protected information environment, it is no longer under the control of an information watchdog. Also the risk of information compromise increases whenever information is "output" in sending it from one information watchdog to another. An abbreviated possible approach to structuring the Device Type grouping is shown in Figure 2.4. In Figure 2.4, the External Output entry refers to output from a device away from the protected information environment, and the Internal Output entry refers to output from a device to another device within the protected information environment (it can also apply to read access at a device). Although a single device can include more than one device type,



each type must be individually controlled by the information watchdog. Some of the control attributes that can apply to entries in the Device Type grouping are:

- Include with the output a label that is a derivative of the IACL, i.e., at the top and bottom of a sheet of paper, a human readable label can indicate who is permitted to view the sheet.
- Encrypt the output using an encryption scheme approved for the type of output. It is assumed that generally an information originator will want his or her protected information to be encrypted but it is possible for the protected information environment to be used for purposes with which encryption would be undesirable. Therefore it is made optional with a default for its use.
- Specify an allocation of the number of outputs. After each output, the allocation number is decremented by the information watchdog. For instance, if the information is a software program, then a set number of copies, whether on diskette or on another computer, can be made.
- A more involved attribute could supply a data format which would apportion the accompanying information into sections of varying sizes. Each section could be assigned its own control attributes.
- As explained in a later section, a communications channel between a recipient and an originator may need to be established before the transfer access or read access of information can occur. This can be requested by an originator by including a reference to its entry in the Originators Link (OL) section of the IPT (to be discussed later), within a control attribute.

#### **2.4.4.3 Need for Standard Control Attributes**

The ultimate in the ability for an IACL to control a device to the liking of an originator, is achieved through program control. A transferred unit of information may contain data and the computer program to process the data. By doing this, the

information unit is supplying to a device a Processing Function validated information usage influence. Alternatively, the IACL may require that the program already exist at a device. Program control allows for flexible control over information.

In one respect, a problem would exist if control could only be achieved through unstructured program control. Protected information is allowed to be aggregated as long as the associated information protection tags do not specify mutually exclusive allowed accesses. The resulting combined information protection tag for the aggregated information must be equally or more restrictive than any of the individual tags. In order to combine the tags, the information watchdog must be able to discern structure in them. The usage states (naming attributes), derive their structure from the IDD. In order for control attributes to be combined, a rule must exist for each control attribute, which determines the relative degree of restrictiveness for all possible values -- a combined control attribute is assigned the most restrictive value of all the values being combined. The approach to control processing functions via program control may not supply the structure needed that would allow control functions to be combined. Hence, predetermined control attributes are probably needed.

A bit pattern was developed which allowed naming attributes to be combined using a general purpose algorithm. Perhaps a coding scheme can also be applied to control attributes so that they can also be easily combined. Otherwise, the full interpretation of the control attributes (which is only required to exist at validated usage states) can be used to combine control attributes and the encompassing IACLs.

#### **2.4.4.4 Default Device Type Controls in All IDD Entries**

In order for IACLs to be more concise, each entry in the IDD can be given a control attribute which can contain a listing of usage influences and corresponding control attributes from the Device Type grouping. All of the usage influences of the other groupings must make use of devices to process information so this feature allows

the administrative body in charge of an entry to specify the default or required output modes and control functions for that entry. If a usage state has a concatenated entry (which indicates many usage influences) then the device type control attribute of the last included entry applies to all of the implicitly indicated usage influences.

#### **2.4.4.5 Focusing Controls**

An IACL can consist of many usage states and some included usage states can be subsets of other included usage states, in the sense that they include additional usage influences. An information originator may purposefully include both of these usage states so that the more narrowly focused subset can have more lenient control attributes than the broader superset.

### 2.5 Sections of the Information Protection Tag

The Information Protection Tag (IPT) has been described as a label which is associated with protected information and which instructs the information watchdog at a device on how to perform certain operations. The IPT and the protected information comprise the Protected Information Unit (PIU). The IPT consists of a number of sections, one of which is the Information Access Control List (IACL). The IACL controls PIU distribution and various information processing functions at a device, and was already discussed in conjunction with the Information Distribution Directory (IDD). The other sections of the IPT are the Identifying Information section and the Originators Link section. The sections of the Information Protection Tag (IPT) are illustrated below:

Information Access Control List (IACL)	Identifying Information (II)	Originators Link (OL)
--	------------------------------	-----------------------

### 2.5.1 Identifying Information Section

The Identifying Information (II) section is a means of notifying third parties of the existence of protected information which may be of interest to them without creating a diversionary channel. The possessor of a PIU, for various reasons, may want to transfer the PIU to other parties. In some cases, assuming the receiving party has the proper (usage state) credentials, the PIU can be transferred without the need for other procedures. In other cases, the receiving party may want to know the general nature of the protected information before it accepts the PIU, especially if it has to pay for it. There are other reasons why a party would not want to blindly accept a PIU. Therefore the contents of a PIU needs to be described in general terms. This general description should be limited or else a paraphrasing process may reveal too much information. This general description should also be standardized so that processing machines as well as humans can easily understand it. Although credentials are somewhat transitory, it may be possible to send this general description to only those parties with the proper credentials. This canvassing approach to finding interest may cause needless communications. The information exchange relationships among parties should be allowed to develop naturally. In order for this to occur, the general description of a PIU can be openly made known at the option of the originators.

A centrally available, official list of information subjects (key words) is needed. When information originators are generating a PIU, they must agree on the appropriately descriptive official subjects. These are included in the II section of the IPT. The fields in the II section are designated as nonconfidential items since copies of this information can leave the protective fold of the information watchdog. The II must as well be contained within the PIU so that the II's integrity can be protected by the originators' cryptographic signatures (as explained further in the next chapter). Other fields within the IPT, such as in the IACL section or the Originators Link section, can be marked as

nonconfidential. When the fields in the II section are written by a modifier (a secondary originator) of a PIU, the protected information section can not be accessible to a user program, otherwise a user program could control the selection of the official subjects based on the contents of the information, thus creating a covert channel with moderate bandwidth.

The nonconfidential items allow discussion about a PIU without compromising its content. Any program (not just an information watchdog internal function) can access and process nonconfidential items. They can be included in widely accessible data bases or exchanged freely among devices. For instance, at a time prior to the transfer of PIUs or even the existence of particular PIUs, devices can enter into information exchange agreements, in which they exchange lists of official subjects (and other nonconfidential items) which they have an interest in. These lists are kept in regular non-IW-protected files. When PIUs are received, modified, or created, the information watchdog can make a copy of the nonconfidential information and place it in a non-IW-protected file. With varying degrees of human intervention, a user program can compare the nonconfidential items from its PIUs with the requests made by other devices. If a match is made and other administrative considerations allow it, the user program can contact the potential recipients to inform them of the existence of the information. The potential recipients if interested, then need to contact the information watchdog at the sending device, as is explained further in the next chapter.

### 2.5.2 Originators Link Section

The Originators Link (OL) section of the IPT provides for a communications channel between an originator of the PIU and all of the PIU's recipients. (It should be stressed here that the list of originators can grow as recipients become originators, as

they add to or massage the received information). The various features of this section can be selected at the option of an originator. The two primary features involve one-way communications from a recipient to originator and two-way communications between recipient and originator.

### **2.5.2.1 Audit Trail**

One-way communications is used to send an audit message to an originator. After a sending device verifies that a receiving device is permitted to receive a PIU but before the PIU is transmitted, an audit message must be sent to those information originators who have:

- included an entry for themselves in the OL section, and
- included a reference (to their entry in the OL section) in the OL control attribute which accompanies the Device Type usage influence to which the information is to be output.

When a PIU is transferred, in terms of communication protocols, all that is required is that the sending and receiving devices can communicate. If they can not communicate, the PIU can not be transferred. Since over time, a PIU can end up in all regions of the diversified network -- having gotten there by many "hops" through the use of possibly many protocols -- to get an audit message back to a PIU originator reliably, requires a standard protocol. (Alternatively, before a PIU is transferred, it could be determined that the receiving device can accommodate the PIU's need for certain protocols for the audit message, but this can get unwieldy.) By a standard protocol, in this case, is meant a system that can take a general message and transfer it anywhere. The postal systems of the world accomplish this for the physical delivery of letters and now based on this paradigm electronic mail (e-mail) has been developed.

E-mail can consist of different interworking systems. An international e-mail standard is the Message Handling System (MHS) which is described in the X.400 [12]

series of CCITT Recommendations. The message structure handled by the MHS basically consists of an envelope and its contents. The envelope contains items which are needed to route the message; key to this is the address of the recipient. The presentation service access point (PSAP) address can be used for the address of an audit message recipient. The audit message can be sent directly to a device in the possession of the PIU originator, or as CCITT Recommendation X.413 [13] describes, the message can be stored in a Message Store provided by a carrier-like organization, until the PIU originator chooses to access the message. An alternate address can also be specified which would direct the audit message to a trusted message bureau in order to impede traffic analysis.

For the MHS, the message content is freely dependent on the application, although a formatted header is available. For the audit message, the contents should include the following fields, the values of which are copied from the corresponding fields in the OL section of the IPT:

- Time stamp at origination
- Sequence number
- PSAP address (of the originator, not a message bureau)

The contents should also include the following fields, the values of which are based on the PIU transfer which is about to occur:

- Time stamp (UTCTime)
- Address of recipient (PSAP address)

The format of the body of the audit message should be standard so that an application program can read all audit messages for various processing tasks. Within the OL section, the originator can supply the public key of an audit message receiving device and instruct that the audit message must be encrypted to provide data

confidentiality. The originator can also request that the audit message be cryptographically signed by the information watchdog about to transfer the PIU. Encryption concepts will be reviewed and further applied in the next chapter.

### **2.5.2.2 Faulty Distributions and Malfunctions**

In addition to making it possible for originators to keep track of the authorized distribution of their information, the audit trail feature encourages compliance with the instructions in the IACL and it alerts an information originator if, for some reason, a faulty distribution is made. The audit trail may not indicate every faulty distribution since the protected information environment, as is possible with any system, may malfunction. A malfunction, including the improper use of the system, should be considered a system-wide problem rather than the problem of an individual. Such problems should be investigated by a central organization although private efforts to understand the problem should be allowed as well. The former is analogous to the police force and the latter is analogous to a private investigator. Once the problem is understood, it should be fixed and the faulty distribution amended.

### **2.5.2.3 Transfer Permission**

Two-way communications gives the information originator the ability to permit or forbid the transfer of the PIU to another device. One of the basic design objectives of the overall system as was discussed in Section 1.3.2, is to allow protected information to be on its own in the sense that it can pass from user to user as long as each transfer is in agreement with the associated information protection tag. This objective is the motivating factor behind most of the design but it should not proscribe an originator of information from making distribution decisions at later dates. This can be accomplished with a modified audit message and with a return approval message from the information originator. In order for the information originator to reach a decision, a communications



channel may also need to be opened with the potential recipient. This approval feature may be of particular value if the originator wants to be remunerated for each transfer (or even for each hard copy output) of the information. The algorithm which determines whether or not access should be granted may not be "mechanical" and so human intervention may be required. The details of the protocol will not be developed in this paper other than that a field in the OL control attribute of the Device Type grouping should indicate whether or not originator approval must be received before a transfer can occur.

#### **2.5.2.4 Modification of an IACL**

It is possible that an IACL which is attached to information may be deemed at a later time to be too restrictive by the originators of the information. The IACL exists to protect the interests of all the originators of a unit of information and an IACL should be able to be modified if all the originators, as specified in the OL section, have reached a new mutual agreement -- the originators should not be bound by the system against their will as to how their information is used. A protocol, not developed here, which would make use of the entries in the OL section, could allow for an IW to attach a new (less restrictive) IACL to an existing PIU.

### 2.6 The Protected Information Unit

In addition to protected information and an IPT, a PIU consists of one more section. This section is called the "receiving device specific instructions" (RDSI) section. The RDSI section allows the receiving device's actions to be under the direct control of the sending device, i.e., if the receiving device is a memory board then the sending device can specify the addresses at which the data should be stored. In contrast the IPT contains instructions of a more general nature specified by the originators of the information to control the actions of all future receivers of the information. The RDSI

by being included in the PIU indicates that it must be protected -- be under the control of the IW including being encrypted with the receiving IW's public key. This is because the RDSI may be formulated when the protected information is being processed and so the RDSI could be encoded in such a way as to represent the protected information. After the receiving device follows the instructions in the RDSI it can discard them. In contrast, as long as the protected information remains in the device, the IPT must be retained.

The three sections of a PIU are shown below:

Information Protection Tag (IPT) or IPT Reference	Receiving Device Specific Instructions (RDSI)	Protected Information
---	---	-----------------------

The term PIU can have a slightly different meaning based on the context of the PIU. During transport, a PIU consists of a message which can be of arbitrary length as distinguished from a packet. The message is made distinct by consisting of a section which either contains an IPT or a reference to an IPT. In the case of a reference to an IPT, the receiving device must have already successfully received the actual IPT. At a device, the various messages relating to the same transaction is called a PIU -- the same IPT applies. The aggregated transactions to which a single IPT applies is also a PIU.

### 2.7 Abstract Syntax Notation One to Define the IPT

The content of the IPT has been discussed. The total picture of the fields which comprise the IPT may have gotten lost in the explanations of them. Therefore, a summary is needed. The fields in the IPT have a structure and the summarizing approach must be able to represent this structure. The structure of the IPT also needs to be captured so that a PIU can be effectively communicated. In Section 1.3.1 it was stated:

In a limited environment, the designations in access control lists, in terms of syntax, are simple. A "fixed" format can be used to code this label information. The format of the label for the everyday world must be flexible so that it can contain various types of directions, including optional directions. Abstract Syntax Notation One (CCITT X.208 [2], X.209 [3]), or a similar language, can be applied to form a flexible access control list label.

One of the advantages that a standard notation offers is that different computers with their own internal ways of representing information are able to interpret incoming data. A standardized interface is a requirement of the information watchdog and standard data representation is one aspect of this.

#### 2.7.1 Brief Background on ASN.1 and its Encoding

In order to make more understandable the structure and encoding of the information protection tag which follows, a brief introduction to Abstract Syntax Notation One is given. A more thorough introduction is given in Computer Networks by Andrew S. Tanenbaum [14] and the standard is written up in CCITT Recommendations X.208 and X.209.

ASN.1 encodes the record structure for transmission by preceding the contents of each field with a field specifying the type of data in the contents field and with a field specifying the length in octets of the data in the contents field. The type of data is specified in a field called the identifier. The identifier also has a bit used to specify if the data field is primitive or constructed. A primitive data field consists of a single data item such as a BOOLEAN, INTEGER, or OCTET STRING. A constructed data field consists of multiple data items (primitive or again constructed). The variations of the constructed type include SEQUENCE, SEQUENCE OF, SET, and SET OF -- a SEQUENCE is an ordered collection of data items, a SEQUENCE OF is an ordered

collection of a single type of data item, a SET is an unordered collection of data items, and a SET OF is an unordered collection of a single type of data item. Unordered in the preceding definitions means that the order of the data items at the receiving computer can be different from the order of the data items at the sending computer and this implies that the order of the data items does not yield meaningful information.

If the structure of an ASN.1 record remained constant then a receiver would have no problem identifying each data item for proper processing. An instance of an ASN.1 record structure can vary due to the DEFAULT and OPTIONAL qualifiers. These can be made use of to form an abbreviated instance of a record structure. This problem with the variability of a record is solved by tagging each data item to uniquely identify it to the receiver. Instead of specifying in the identifier field the type of data item which follows, i.e., INTEGER, a number tag can be used. There are four types of tags -- UNIVERSAL, APPLICATION, PRIVATE, and context specific. The UNIVERSAL type was implied in the previous paragraphs and describes the type of data in the contents field, i.e., INTEGER, SEQUENCE. The UNIVERSAL type is understood in an ASN.1 data item representation if another type of tag is not stated. The APPLICATION tag consists of the word APPLICATION followed by a number, all in brackets. It is used to identify, with number tags, data items within a particular OSI application layer protocol. Within a particular application, an APPLICATION number can only be assigned once. The PRIVATE tag is used in a similar manner but applies to non-OSI standardized applications. The context specific tag consists of a number in brackets. A context specific tag number can be used more than once in a given structure -- the number along with the context in which it is found is used to identify the received data item.

Since a tagged data item can be identified with the tag number, the type of data item, i.e., INTEGER, is redundant information in identifying a received data item. The

type can be omitted from the encoded stream by preceding it with the word **IMPLICIT**. This removes a level of construction which when applied throughout an ASN.1 structure can reduce the size of the encoded stream.

The information protection tag structure is expressed in ASN.1 in Appendix B.

## **CHAPTER 3**

### **COMMUNICATIONS BETWEEN DEVICES**

#### 3.1 Introduction

A communications channel of some sort connects all devices in the protected information environment and is needed with various aspects of the formation and use of PIUs. Besides being used for the transfer of PIUs, a communications channel is needed to reach an agreement among all parties involved in a transaction as to the contents of a PIU including its IPT. A communications channel is also needed for a potential recipient of protected information to transfer its device credentials to a sender of protected information in order for it to be compared with the IACL.

#### 3.2 Public Key Cryptography for Secure Communications

The channels which connect devices must be secure. Secure communications has a number of aspects. These aspects can be accomplished with public key cryptography as first proposed by Diffie and Hellman in 1976 in their paper, "New Directions in Cryptography" [5]. Public key cryptography has an asymmetric key scheme with a public key and a private key. Each key, public or private, has the same mathematical functionality so either one can be used for encryption or decryption. Their differences result from their private or public status. Private keys should be held as tight as possible whereas public keys can be distributed widely such as through the use of a public data base. Information can be kept confidential during transmission by encrypting it with the recipient's public key. The originator of information can be authenticated by signing the information with the use of the private key.

Although public key encryption offers convenience and the ability to authenticate a message, it takes 100 to 1000 times as long as other encryption methods. To get around this, the public key can be used to encrypt the key of a faster symmetrical encryption scheme like the Data Encryption Standard (DES). Once the other party securely receives and decipheres the DES key, all remaining confidential communication between the parties can be encrypted using the symmetrical key.

CCITT Recommendation X.509 [7] which is part of the series of recommendations describing a public/private directory data base, offers some valuable features that are related to public key encryption. Basically, it provides a way to distribute public keys. To do this it defines certification authorities which lend trust to the distributed public keys. If a public key in a widely accessed data base could be switched with a phony public key, and if the owner of the phony public key could intercept all messages headed for the valid recipient, then he could decipher all messages and possibly carry on a seemingly valid communication with the other party. The certification authority, which must be trustworthy, encrypts or cryptographically signs public keys with its private key. The result is called a certificate. A distributed certificate which can only be deciphered with the certification authority's public key, gives credence to the encrypted public key. Just as the Information Distribution Directory is decentrally administered, so can be the certification authority. For intracompany and possibly some intercompany communication, the certificates can be administered internally by the company, leading to a higher level of trust.

### 3.3 Aspects of Secure Communication

CCITT Recommendation X.509 [7] describes the different aspects of secure communication and how these can be implemented using public key encryption. These will be reviewed here and will then be related to the needs of the protected information environment:

### 3.3.1 Data Confidentiality

This is concerned with protecting information from unauthorized disclosure. It is accomplished by encrypting the message with the recipients public key. Only the recipient (the possessor of the private key) can decipher the message.

In the protected information environment, data confidentiality whether with an asymmetric or symmetric key is an option that originators of a PIU can selectively require based on the type of information transfer or output which is to occur. These requirements are stated in an IACL, in the control attributes of a Device Type usage influence. The recipient's asymmetric or symmetric key, is included in the device authentication token (discussed in Section 3.4.8) which is transferred to the sending device immediately prior to a transfer of a PIU.

Data confidentiality can also be applied to the audit message. As delineated in Appendix B, the audit-confidential-required field can optionally be included in the OriginatorInfo sequence. This supplies the algorithm and the originator's public key to be used to encrypt the contents of the audit message. If the audit message is to be sent to a trusted clearinghouse by specifying an alternate address, then the public key must be that of the clearinghouse's receiving device.

### 3.3.2 Data Integrity

This is concerned with protecting a message from alteration during transmission. Data integrity is accomplished by giving a transmitted message a characteristic which can indicate if a message has been altered. This characteristic is a cryptographic signature. To generate this signature, the message is first input to a hash function which produces a relatively short reproducible bit string. A change to the message will generally produce a different bit string; i.e. the probability that the same bit string results is very small. The bit string is encrypted with the sender's private key. The recipient inputs the received message to the same hash function. Alteration has occurred if the



resulting bit string does not match the deciphered bit string. An encrypted time stamp and/or sequence number can accompany the message to prevent the message from being reissued.

In the protected information environment, data integrity is enhanced by allowing each originator of a PIU, whether a primary originator or a secondary originator, to sign the PIU. The signature is placed in the `piu-integrity-signature` of the `OriginatorInfo` sequence. The hash function can be applied to the protected information and the IPT, minus the `piu-integrity-signatures` for all of the originators. As delineated in Appendix B, the `piu-integrity-signature` consists of the `ValidatingSignature` construct. This construct will be explained in Section 3.4.2.

Of course the PIU, both the protected information and the IPT, can be processed in different ways allowed by the IPT including being aggregated with other PIUs. The original or preceding `piu-integrity-signatures` which should remain with the changed PIU will no longer correspond to the PIU -- only the signatures of the originators of the most recent version will correspond. The value of the preceding signatures is not destroyed or diminished though since the PIUs that do correspond to these signatures still can exist in the network. If integrity is important, the participants in any organized transfer of information can communicate at the time or set up procedures to save or exchange preceding PIUs. The vestigial signatures in the later PIUs verify the correct course of evolution of the PIU.

The integrity signature helps by revealing alterations to the PIU but it is still possible for the IPT to be stripped away from the protected information, with the possible substitution of a false IPT. The encryption of a PIU can aid with integrity as well as confidentiality. In order for a PIU to remain protected its IPT must remain logically associated if not physically associated with the information. Physical association can be accomplished by encrypting the IPT and protected information as a

single unit with the receiving information watchdog's public key (or with a symmetric key). Certain transfers may be accomplished more efficiently if the IPT can be transmitted once -- each unit of information subsequently transferred would not be burdened by the overhead of the IPT. By encrypting each unit of information with the receiving information watchdog's public key, the information can securely reach the other device. At the receiving device, the information watchdog needs to know which IPT is logically associated with the received information before any processing can be performed other than storage of the information in a buffer. The tie between IPT and information is accomplished by the receiving information watchdog transferring to the sending information watchdog a token containing a sequential number (IPT reference) and an expiration date encrypted with its private key. This short token can substitute for the IPT in an encrypted PIU.

An originator can also optionally request that any audit messages sent to it be signed so that their integrity can be ensured. This request is made with the audit-integrity-sig-required field of the OriginatorInfo sequence. The signature fields in the audit message would need to include all those of the ValidatingSignature construct delineated in Appendix B.

### 3.3.3 Non-repudiation

This is concerned with the denial of transmission by the sender of a message. There are a number of commercial transactions which involve a signed document. The signed document gives certain protections to the recipient. An example is a bank check. Non-repudiation (associating a signature with a message), is accomplished by either the originator encrypting the entire message or the result of a hash function with his private key. The recipient of a signed message should keep a copy of the encrypted message to be able to demonstrate at some future time, if need be, that the deciphered message under dispute can be obtained from the encrypted message by using the sender's public

key. If a signed message is claimed to have been fraudulently sent because a private key has become known to the public, the burden of responsibility should generally be on the key owner.

In the protected information environment, non-repudiation can be accomplished with the same signature used for data integrity. Section 3.4.7.4 mentions the possible need for a data base of stolen IWDs which would counter the fraudulent denial of service problem.

### 3.3.4 Access Control

This deals with restricting access to the use of resources, to only those who are authorized. This aspect of secure communications does not necessarily rely on cryptographic techniques.

In the protected information environment, the matching of a PIU's IACL with a device's credentials accomplishes access control.

### 3.3.5 Peer Entity Authentication

A method is needed so that what an entity at one end of a communications channel purports to be, can be authenticated. Since a private key is to be only known by its owner, a message encrypted immediately before being sent over a communications channel, can authenticate the identity of the sender.

For the protected information environment, authentication is accomplished through an independent process which validates the presence of an information usage influence at a device. All such validated usage influences make reference, via the device ID, to the same public key. The public key, in essence, creates an authenticated channel to the IW at the device. This process is described in greater detail in the next section.

### 3.4 Authentication of the Receiving Device

#### 3.4.1 The Importance of Valid Device Credentials

PIU distribution is controlled with a two tiered approach:

##### **3.4.1.1 At a Receiving Device**

The first tier is concerned with the credentials of the recipient of protected information. For this, minimum reliance is put on the trustworthiness of the recipient device. Instead, each validated usage influence is included in a certificated token which includes the device's ID. In this way trusted independent validating organizations can tie the validated usage influences to a device. A device in this sense is just an amalgamation of validated usage influences. Even if an IW is not in control of all the processing of protected information that is occurring at a device, at least the device has the traits desired by the originators of the received information.

##### **3.4.1.2 At a Sending Device**

The second tier is concerned with the trustworthiness of a device in its sending mode. As discussed in the next chapter, an information watchdog resident device must be tamper proof. If a device is not trustworthy then protected information once received can be sent anywhere regardless of the credentials of a receiving device. For this system to work as planned, information watchdog resident devices must be trustworthy. But if otherwise, the system can continue to function, since as long as the authenticity of credentials holds-up, protected information can be directed to only those devices which are trusted. The selection of allowed recipients of information can depend on the level of sensitivity of the information.

### 3.4.2 The Certificated Token

The concept of the certificated token is made much use of in the authentication process. In the broad sense, a certificated token is any group of fields which has its integrity protected through the use of a cryptographic signature. The ValidatingSignature ASN.1 field in Appendix B was applied there to protect the integrity of a PIU. It can also be used to form a certificated token of a usage influence. It will be reexpressed in the notation of Table 1 of CCITT Recommendation X.509 [7], where it is stated that  $X\{I\}$  indicates "the signing of I by user X. It consists of I with an enciphered summary appended.":

$$\text{Certificated Token} = V\{ \text{various fields, CA}\{ V_{\text{validating info}} \} \}$$

where the certificate:

$$\text{CA}\{ V_{\text{validating info}} \} = \text{CA}\{ V_p, V_{\text{hf}}, V_{\text{ea}}, V_{\text{did}}, V_{\text{ac}}, \text{TP}, \text{CA}_{\text{sid}}, \text{CA}_{\text{did}}, \text{CA}_{\text{sn}} \}$$

where:

V signifies the validating device, and

$V_p$  is its public key,

$V_{\text{hf}}$  is its hash function identifier,

$V_{\text{ea}}$  is its encryption algorithm identifier,

$V_{\text{did}}$  is its device ID code, and

$V_{\text{ac}}$  is its authority code.

TP is the time period during which the key pair is valid.

CA signifies the certification authority device, and

$\text{CA}_{\text{sid}}$  is a signature ID code,

$\text{CA}_{\text{did}}$  is its device ID code, and

$\text{CA}_{\text{sn}}$  is the sequence number for the certificate,

"various fields" pertains to items whose inclusion are dependent on the particular type of information being certificated. The items which are included within usage influence tokens are specified in Section 3.4.7.

Comments on fields:

- In the ASN.1 version in Appendix B,  $V_p$ ,  $V_{hf}$ , and  $V_{ea}$  were included in the SignatureCryptomethods construct. Similar fields exist for the CA. They can either be explicitly stated or as is indicated above, a signature ID code,  $CA_{sid}$ , can reference this information. There are primary certification authorities, whose hash function identifiers (and hash functions), encryption algorithm identifiers (and encryption algorithms), and public keys must be securely embedded in every information watchdog during manufacture -- in the general case this information would exhibit its veracity from its highly public status, but the information watchdog being a machine requires that this information be securely implanted during manufacture. The  $CA_{sid}$  would reference one of these embedded signature methods. As described in X.509 [7], certificates can be chained (a V certificated by a CA, can become a CA in relation to the next V) and so the signature information for secondary certification authorities can as well be stored in an information watchdog. The chain would need to start with a certificate which uses a  $CA_{sid}$ , though.
- The device ID codes,  $V_{did}$  and  $CA_{did}$ , tie a public key to a device. A certificate  $CA\{\dots\}$  provides integrity in regards to the distribution of a public key, and the device ID indicates which device has the corresponding private key. The existence of a certificate also indicates that the private key was securely implanted within the device. Certificated usage influence tokens contain the device ID, so the certificate relates a public key to these tokens.

- The validating authority code,  $V_{ac}$ , indicates the type of information which can be validated by  $V$ . In most cases, the only authority given to a device will be the authority to sign and encrypt information which it generates. Of particular importance to this section, is the authority to validate the presence of a usage influence at a device. These authorities must be independent and trustworthy. Depending on the usage influence being validated, they can use different techniques to perform the validation. These techniques can involve audits, examinations, automated processes, etc.
- The time period of validity,  $TP$ , consists of a starting time and an ending time during which the public/private key pair can validly engage in the authorized cryptographic activity. A bounded duration is required for the authority to validate usage influences. For a typical information processing device, issues concerning the period of duration for its key pair are discussed in Section 4.2.3.1.
- The sequence number,  $CA_{sn}$ , can help keep track of the certificates issued by a certification authority.

### 3.4.3 Access Rights are Device Centered

In a more limited computer environment, a user presents a user ID to a computer system, and based on the user ID certain access rights are granted. In the Protected Information Environment (PIE), emphasis is shifted from a single user ID to a single device ID, which is placed in all usage influences which a device has been validated for. Based on the combination of usage influences with the same device ID, certain access rights are granted to the device.

In a more limited environment, an administrative organization can be in control of all aspects of processing, i.e., location of devices, computer programs used, assignment of personnel to tasks. All that remains is the identification (and authentication) of the user at the computer. In the PIE, a device's position as the center

of processing is emphasized; a device (or a usage state at a device) needs to identify its unique character, to protected information, in terms of its validated information usage influences.

#### 3.4.4 Validated Usage Influences Belong to the Device

The validated usage influences at a device can be thought of as belonging to the device rather to an "application" at the device. Before an application can be allowed to process information though, it must be determined by the information watchdog that at least one of the usage influence combinations found in the form of usage states of the information's IACL are present with the application.

It may be possible for a device to have a sufficient selection of usage influences to receive a PIU which can not be accessed by any application at the device due to a lack of the right combination of usage influences with an application. For instance, a device can have a certain computer program and a certain user which taken together is enough for the device to receive the information, but at the device, that particular user is not allowed to use that particular program. This is an internal matter for that device, the information originators haven't prevented this access. The certificated usage influences at a device can be placed into different usage states which make up a device's credentials. The usage states can indicate the allowed combinations of usage influences at a device, thus preventing the transfer of a PIU that the device does not choose to process.

#### 3.4.5 Validation of Usage Influences at a Device

The Information Distribution Directory lists the identified information usage influences. Each usage influence indicates an influence on information usage. The presence, rather than absence, of a usage influence at a device is used to determine a device's access to information, for the following reasons:



- Since human initiated action may be needed to validate a usage influence, including a possible payment for each validation transaction cost, a motivating factor is for a validated usage influence to make more information accessible rather than less.
- The presence of a usage influence at a device may be considered by the owner of the device to be a private matter. The owner may be willing to forgo access to certain information, in order to not make known the presence of a usage influence.

An analogy can be made between PIUs and children. The emphasis is not on keeping children (PIUs) away from bad influences, but on only allowing them to hang around with acceptable influences. These influences should be as narrowly focused as possible. Ideally this should not just be a matter of definition but of practice. A realized usage influence should ideally not be allowed to have other usage influences tag along. For instance, a computer program, or a device, can be factored so that the information watchdog is able to give only the specified usage influence access to the information. When these usage influences are validated, purity of function must be checked for. On the other hand, there can be usage influences which can not be factored. For instance, a person may have a number of work related roles -- good intentions and a specified usage influence can direct a person's mind set but it is difficult to block-out other areas of thought. In any case, narrowly focused usage influences can better restrict the distribution of the information.

Each entry in the Information Distribution Directory can have its own validation approach. It is expected, though, that all entries (on the same tree) within a usage grouping will be validated using the same approach. Each approach should be as effective as is reasonably possible. A usage influence is validated by validating each

entry that it consists of. The validation of usage influences must answer the need described in Section 1.3.1:

In a limited environment, trust can be placed in an administrator to assign the appropriate designations to users. This is needed so that the designations in an access control list associated with information will be adhered to. In the everyday world this administrative function still needs to be performed but of necessity must be accomplished in other ways. Some equipment, limited to performing certain functions, may be able to be sold with a preconfigured security label. Other cases may require an independent verification process in order to determine the appropriateness of labels assigned to entities. This validation can then be indicated by the cryptographic signature of an entity's label.

#### 3.4.6 Considerations for Selecting the Time Period of Validity of a Usage Influence

Each token of a validated usage influence contains the time period (TP) of its validity. A PIU sending device must check that the time period of each relevant device token of a receiving device has not expired before sending a PIU; the same must be done by a device prior to its internal accessing of a PIU. There are a number of basic approaches with which to select a time period, two of which are discussed below.

##### **3.4.6.1 Real Time Authentication**

With real time authentication, the TP field is set to only take into account transmission time. After the validating authority completes its task, the device token may pass back to the validated device, and may then be sent to an information sending device. The transmission time, which results in the non-instantaneous receipt of a validated device token, is estimated for in the TP field. The benefit of real time

authentication is that the actual state of a device has little chance of diverging from the device tokens which represent it.

In some cases, a validating authority may also be in control of the assignment of a usage influence, for instance, a business firm's relationship with its employees. The controlling organization would usually keep a data base of the current status of such a relationship. Reference to such a data base provides a simple real time mechanism to issue a device token. In other cases of device authentication, in addition to a real time reference operation, a real time validation procedure will be needed.

### **3.4.6.2 Estimation of Time Period of Validity**

By using the TP field to state an estimated time period for the validity of a usage influence at a device, the frequency for the performance of the validating procedure decreases. Time for transmission must still be considered but now the selection of the time period, by the administrating body of the usage influence, can be influenced by additional factors. For instance:

- Within how much time after its assignment is it likely that the information usage influence will no longer be valid?
- What is a practical period of time in which to force the update procedure?

The problem with this approach is that the actual state of a device may diverge from the device tokens which represent it. The advantage is that the expense and overhead resulting from validation transactions should be lower. Validated usage influences are required prior to each transfer of information and each usage state switch at a device. If a device is consecutively transferring PIUs to another particular device or if a device is alternating between the same usage states, then requiring that usage influences be validated prior to each transfer or switch may cause unjustified overhead. Instead, the estimate for the time period in which it is likely that a device token will still accurately reflect the device can be set conservatively.

The selection of a time period is further complicated by aspects particular to some usage influences. For instance, some usage influences, such as the fact that a certain software product was purchased for a particular device, can have very long or possibly an unlimited time period of validity.

### 3.4.7 Examples of Usage Influence Validation Techniques

In Subsection 3.4.2 of this section, the fields in a certificated token were given. The item described as "various fields" gets its members in regards to information usage influences based on the particular usage influence being validated. Typical members are UI for the usage influence code which comes from a path of entries in the Information Distribution Directory, TP for the time period during which the UI is valid, and ID for the device ID. Generally the last signature applied to a certificated token is that of the validating authority. When the device ID can not be placed within this token, the device itself can wrap the validating authority's token and the device ID within its own token. It is required that all certificated tokens sent to another device contain the device ID in order to tie the token to the device.  $D\{\dots\}$  will represent a token signed by the device containing the usage influence. Some validation approaches, by usage grouping, along with the corresponding members of the "various fields" section are given:

#### **3.4.7.1 Processing Function**

The installation of software on a computer creates a usage influence which can be validated. Software validation requires that the software be reviewed by an independent auditor. Its purity of function should be verified. For mass market software products, this verification process can be performed once for each released version allowing for economies of scale. For in-house or custom software, the same process can be used, although the verification effort may be spread over fewer copies. The auditor should then form a certificated token to accompany the software module which would

include the appropriate usage influence and a signature which is applied to a hash function taken of the software module. Whenever the software module is loaded for processing, the information watchdog would verify the validity of its usage influence by checking the signature.

If the software is initially loaded onto a device via some form of communications channel, with an IW protected device acting as the server for a validating authority, then the device ID can be included in the token formed by the validating authority. Otherwise, an exception to this scheme can be made where the IW would create its own certificated token, containing its device ID and the auditor's token to indicate that the usage influence is present at the device.

It should be mentioned that within the Protected Information Environment, software is generally protected information. It may, in addition, be an information usage influence.

Token = V{ ID, TP, UI, Signature of hash function of SW code, CA<sub>v</sub>{...} } or possibly

Token = D{ CA<sub>d</sub>{ ID, ...}, V{ TP, UI, Signature of hash function of SW code, CA<sub>v</sub>{...} } }

### **3.4.7.2 Device Type**

Each device is configured in a factory (a discussion of the meaning of a device is given in the next chapter). Each implemented function in a device, as identified in the Device Type grouping, must be individually controllable by the information watchdog. An independent auditor, working in conjunction with the manufacturer, can supply a certificated token, for each validated usage influence, for inclusion in the information watchdog. The information watchdog must check for the presence of the Device Type token before activating the associated device function.

Each addressable memory location may act as a port to a certain type of device function, i.e., bit mapped displays. Each memory location, through the specification of address ranges, is assigned a Device Type usage influence. These assignments are entered into certificated Device Type tokens -- one for each validated Device Type usage influence.

$$\text{Token} = V\{ \text{ID}, \text{TP}, \text{UI}, \text{Applicable memory location or port ID}, \text{CA}_v\{\dots\} \}$$

### **3.4.7.3 Device ID**

An independent auditor must oversee the manufacturing process of information watchdog resident devices. The device ID is included in a certificated token which contains the public key of the device. The auditor will issue this token if the private key of the device was securely implanted in the device and other aspects of the device meet requirements (further discussed in the next chapter). All other tokens contain the device ID, and this token is sent out along with any other token to indicate the public key belonging to the device which owns the tokens.

$$\text{Token} = \text{CA}_d\{\dots\}$$

### **3.4.7.4 Person & Work Related Role**

Some usage influences, such as those belonging to the Person and the Work Related Role usage groupings, ascribe to a person. If a person uses certain devices, then the validated usage influences for these groupings should be able to be transferred to those devices' information watchdogs. But more importantly, these validated usage influences belong to a person and should be physically associated with a person, both in terms of being able to be carried on a person and as being bound to a person's physical attributes. The carrierability of usage influences can be accomplished by having them stored in a smart card which allows for portability with particular ease. The boundability of usage influences can be accomplished with biometric techniques.

An independent organization should capture one or more biometric identifiers of a person and assign an ID code to them -- a usage influence within the Person grouping. The ID code can be much like a social security number. Both the ID code and the biometric identifiers are included in the same certificated token. The smart card merely acts as a standard and convenient way to carry this token around. For reasons to be explained later in this chapter, a smart card is also needed as an information watchdog protected device. There is no reason why both functions (and possibly other unrelated functions) can not share the same smart card.

When a person wants to be validated for another personal usage influence, verification is carried out by an independent organization. The organization would perform the biometric procedure to verify that a particular Person token belongs to the person who is physically present. From the Person token, the ID code would be read and placed in the new personal usage influence token. This token can as well be carried in the smart card.

For the Work Related Role usage grouping, a licensed job provides a clear example of a validated usage influence from this grouping. The licensing procedure for a job skill provides the verification. The procedure can follow the normal steps (with biometric identification possibly used at various steps, i.e., at an exam), and at the end of the procedure, a certificated token would be formed.

A personal validated usage influence can be used in the dormant state or the active state. In the dormant state, the validated usage influence is present at a device but its owner is not. A device's credentials contain the dormant state so that information transfers can occur without the presence of a person. Once a PIU is at a device, a Person control attribute can require that the person be present to initiate any processing. For a personal validated usage influence to enter its active state, the person, with prompting from the information watchdog, must indicate his or her presence at the device by

engaging in the biometric identification procedure. This procedure must also be carried out, in order for a personal validated usage influence to be transferred to another device (where it can remain dormant). Of course, biometric identification procedures, which may be conducted in private, must not be able to be bypassed.

A person's biometric identifiers and ID code are not secured information. This makes it easier for an imposter to bypass the biometric identification process in order to enter a person's ID on a device. To improve the integrity of this information, the person to whom the biometric identifiers apply can go to a trusted independent organization where the biometric identification process would be performed. The result would be a certificated usage influence token signed by the independent organization which would include the person's ID and the device ID to which the token will later be transferred.

The use of an IW protected device by an unauthorized person is secure up to the point that it displays information without the requirement that an intended recipient indicate his or her presence at the device. If biometric techniques are not full proof then the control that a Person usage influence be in its active state can be bypassed. This may require that a central data base of lost or stolen IWDs be referenced prior to the transfer or access of a PIU which has an active Person usage influence in its IACL -- such a function should be planned for. This also lessens the fraudulent denial of service problem.

The use of a smart card to positively assign traits to individuals in the form of validated usage influences can be carried too far and result in the substitution of recorded information for a person's being as expressed in a more personal manner. Genetic code, religion, and aptitudes are some personal traits that could be converted into validated usage influences. A person may desire not to be so validated but societal pressures may exist. The central administrative body of the Information Distribution Directory can exert influence to prevent or at least moderate this potential problem.



Token= V{ Biometric identifiers, TP, UI, CA<sub>v</sub>{...} }

or

Token = V{ ID, TP, UI, CA<sub>v</sub>{...} }

### **3.4.7.5 Location**

The location of a device is transitory and so requires an update process with a certain degree of temporal resolution. Location also must be determined with a certain degree of spatial resolution. Regions are defined by borders. Within borders, spacial resolution can be gross, but in the vicinity of borders, spatial resolution can never be too fine.

An information watchdog needs to determine its location based on tamper proof input. One possible approach could use cellular transceivers. The key is for a timed communications channel to be established. The device can send to the transceiver its certificated device ID which includes the device's public key, encrypted with the public key of the local transceiver. (The public key of the local transceiver can be distributed in the form of a certificated token so that it can be trusted by an information watchdog.) The transceiver would then initiate a round trip communications sequence in which it would send to the device a packet encrypted with the device's public key consisting of a random number. The device would then decipher the packet and send to the transceiver a packet encrypted with the transceiver's public key consisting of the same random number. The random number ensures a sequential pattern with each leg of the round trip communications. If the elapsed time of the communications is under a certain value, then the transceiver can be assured that the device is present within its cell. It would then form a certificated token consisting of the device ID, location, and time period for validity. The same general approach may be able to be accomplished with the use of wire line communications. A more complicated scheme using multiple transceivers could verify the location of a device with greater resolution.

Since time is known at a device, a one-way GPS-like location service could be used. Each certificated location token could contain the current universal time. Validity would be ascertained if the difference between the device's time and the token's time were less than a certain value based on transmission time. This approach has the disadvantage that the device ID is not included in the certificated location token by the validation authority but has the advantage that since the communications channel is one-way, the design requirements can be less stringent.

$$\text{Token} = V\{ \text{ID}, \text{TP}, \text{UI}, \text{CA}_v\{\dots\} \}$$

or possibly

$$\text{Token} = D\{ \text{CA}_d\{ \text{ID}, \dots \}, V\{ \text{TP}, \text{UI}, \text{CA}_v\{\dots\} \} \}$$

#### **3.4.7.6 Time**

Since time is universal, this is a usage influence which is not sent from one device to another as part of device credentials. Time can be included as a usage influence in an IACL and so it needs to be known at a device. As explained in Section 4.2.1, a reliable steady power supply is needed. A clock would need to be installed in the device and set in the factory and the steady power supply would keep it running.

#### **3.4.7.7 Line of Business**

This requires an on premises independent audit. A line of business can be factored in that a specific device can be assigned to a specific business. An auditor can, with some degree of assurance, attest to the role of a device in the Line of Business grouping and assign a usage influence. The auditor can then create a certificated token which can be tied to the device by including the device's ID, but there is nothing which can tie the device to a line of business other than periodic audits. Therefore, to force a periodic audit, particular reliance is placed on the time period of validity which is included within each certificated token. This of course does not guarantee that the

device and hence the information it receives is only exposed to the information originators' permitted influences in the way of a line of business.

$$\text{Token} = V\{ \text{ID}, \text{TP}, \text{UI}, \text{CA}_v\{\dots\} \}$$

### 3.4.7.8 Pledge Approach

Another approach to validating usage influences is to use a pledge. Here a person at a device pledges that a usage influence exists at a device. The pledge can be used in conjunction with validation techniques for which results can not be guaranteed.

$$\text{Token} = D\{ \text{ID}_{\text{of person}}, \text{TP}, \text{UI}, \text{CA}_d\{ \text{ID}, \dots \} \}$$

### 3.4.8 Transfer of Device Credentials from Receiving to Sending Device

In order to control better the dispersion of protected information, the matching of an IACL with device credentials is done at the sending device rather than at the receiving device. Since validated usage influences can change instantaneously (location, for instance), device credentials should be formed immediately before the transfer is to occur, and be sent directly from the receiving device to the sending device. The packet transferred will be called a device authentication token (DAT) and will contain the following information:

- certificated usage influence token(s) -- these are placed into different usage states to form a device's credentials. The device ID token must be included in at least one usage state so that the device ID which is found in all tokens can be associated with the public key of the receiving device.
- an optional symmetric key and algorithm identifier -- at the option of the receiving device, the PIU can be encrypted by the sending device with a symmetric encryption scheme. This can save time as encryption done with an asymmetric scheme can take longer.

The DAT is signed with the receiving device's private key to ensure the integrity of the data. This unit is encrypted with the public key of the sending device in order to ensure the confidentiality of the data including the confidentiality of the symmetric key. It is then transferred to the sending device where the IACL and the device credentials can be compared.

For some types of information transfer, it may be more efficient for the information sender to be able to access a central data base of validated usage influences in lieu of getting this information directly from the receiving device. The device to which the usage influence belongs would need to voluntarily submit (on a periodic basis) selected usage influences to the data base(s). This would allow for the equivalent of a mass mailing, or allow for the transfer of information via an intermediary storage facility or physical medium of storage, when a device is not generally kept on-line. The integrity of communications with such a data base would need to be maintained.

### 3.5 The PIU's Place in the Open Systems Interconnection Reference Model

Before a PIU can be placed on a physical medium to be transferred from one device to another, certain communications related operations, applicable to the communications needs of all types of messages, must be performed on the PIU message. Some of these operations may be packetization, generation of an error detection and correction code, encoding of data, and encryption. As was previously discussed, the PIU needs encryption for confidential communications and the encoding of its fields into a notation such as ASN.1 so that it can be commonly understood.

Open Systems Interconnection (OSI) provides a practical standard for communications as well as a good conceptual framework for discussing communications related operations and it will be related to the needs of the PIU. An excellent in-depth discussion of OSI can be found in the book Computer Networks by Andrew S.

Tanenbaum [14]. In this section a brief sketch of particularly relevant aspects of OSI will be given. OSI consists of a Reference Model (CCITT Recommendation X.200 [15]) which describes a basic architecture to facilitate communication between computers, especially between computers of different designs and by different manufacturers. OSI consists of many other standards which fill in the details needed to accomplish this goal.

### 3.5.1 OSI Basic Architecture

The basic architecture consists of seven layers where each layer performs a number of related functions to effect a desirable aspect of the communications channel. The seven layers are shown in Figure 3.1. The main functions of each layer are specified in CCITT Recommendation X.200. Each layer performs communication services for the layer immediately above it. Information passing between layers occurs at Service Access Points (SAP). The SAP at a layer acts as a port for communications with the next higher layer. For instance, a Presentation Service Access Point (PSAP) was suggested in previous sections as being an address to which PIU communications can be directed. The information passed consists of a Service Data Unit (SDU), which is information to be communicated, and Interface Control Information (ICI) which instructs the other layer on how to service the SDU. The goal behind the activities of each layer is twofold -- carry out the instructions of the layer above and successfully communicate with a peer entity (on the same layer) at another computer. To communicate with a peer entity, a layer must make use of the services of the layer below it, thus causing a daisy chain through the seven layers. As an SDU passes from one layer to the next, information (a header) needed to communicate with the peer entity at the other device is attached to the SDU. The header plus SDU is called a Protocol Data Unit (PDU); when a PDU is passed to the next lower level it becomes an SDU.

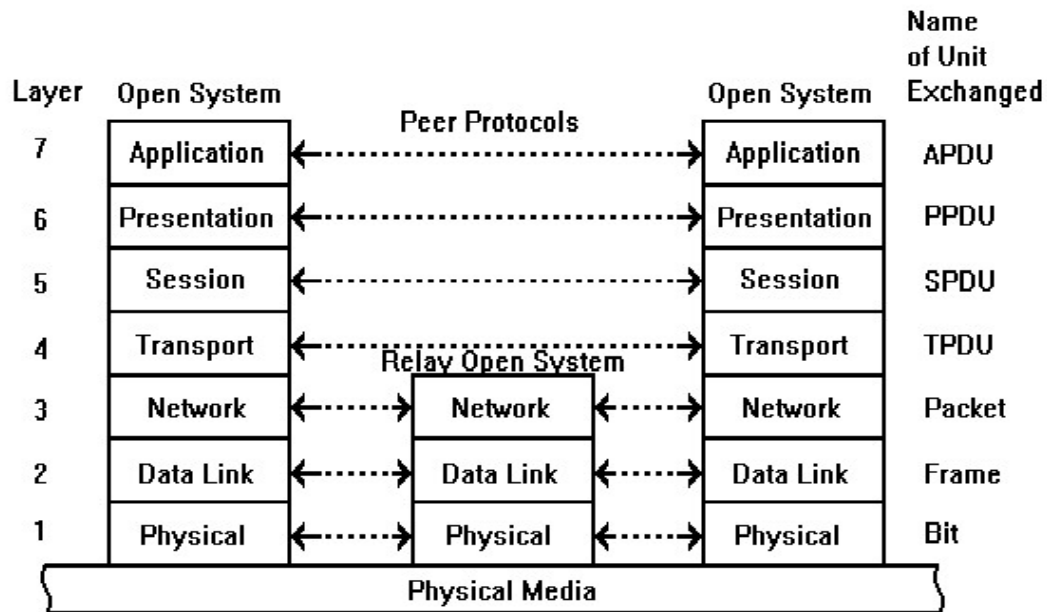


Figure 3.1 OSI Seven Layer Architecture

As indicated in Figure 3.1, at the transport layer and above, communication occurs between end systems. Whereas at the first three levels, communication can occur directly between end systems or can be routed through a subnetwork consisting of one or more relays.

### 3.5.2 The IACL at the Application Layer

The IACL as described, is a way to restrict the routing of protected information among end systems which can be thought of as relays operating at the application layer. As indicated in Figure 3.1, the unit of data exchanged between application peer entities is the Application Protocol Data Unit (APDU). A PIU is formed in the application layer and most of its information is placed in an APDU (as discussed in the next section some of its information may pass to the lower layers). A versatile way to define and encode

the contents of an APDU is by using ASN.1. This encoding can be self-contained or can be done in conjunction with an application layer protocol that offers various helpful services.

A self-contained encoding can be carried out with the Reliable Transfer Service Element (RTSE). Here an entire PIU can be formed and placed in the "APDU" parameter of the RTSE's TRANSFER command. In addition, the application layer must pass to the presentation layer, an ASN.1 identifier. For a connectionless channel, this can accompany the PIU; for a connection-oriented channel this can be included in the RTSE OPEN command. If the ASN.1 representation given in Appendix B, of the IPT is encoded, then certain fields would be given tags to identify them to a receiving device. A family of tags used to encode a particular application is called a context. The presentation layer must be told of the current context, through the ASN.1 identifier, so that it can apply the proper tag to each data item passed to it.

The encoding of a PIU can be done in conjunction with an application layer protocol that offers various helpful services. One such protocol is the Message Handling System of the X.400 [12] series of CCITT Recommendations. Instead of offering a blank APDU, it provides a preformatted structure for transferring information. Just as with postal mail, the major components of the MHS message are the envelope and the contents. The contents in turn consists of the body and the header. All of these parts are defined using ASN.1 so there is flexibility in their make-up.

The header contains fields that inform and direct an end user on how to handle the body of the message. Some header fields are originator, reply time, and subject. The header field sensitivity can be defined using ASN.1 to have an option of specifying a protection tag. The IPT could drop right into this place.

### 3.5.3 The IACL at Other Relay Layers

Since relays can exist at the network, data link, and physical layers, it may be desired that the route taken to transfer a unit of information be controllable to protect information. The reason for this may be that:

- The information is not encrypted or more likely the information is encrypted but redundancy in security is desired in case the encryption methods are compromised.
- The end parties communicating are concerned about their transmissions being subject to traffic analysis.
- Other non-information protection issues exist, such as the cost of transmission may vary depending on which transmission paths are selected.

A distinction can be made between end system relays, and routing relays. (The latter category also includes repeaters, bridges, and gateways). In both cases, information is transferred from device to device. With end system relays, information is pulled to satisfy the processing needs of the receiving device (this is the type of information transfer primarily discussed throughout this paper). With routing relays, information is pushed so that it will eventually reach an end system destination. Other differences between these two types of relays may be a matter of degree. For instance, devices within both types of relays enter into relationships with other devices. The relationship between routers may be more consistently static than that between end systems since routers perform a very narrowly defined function. This may influence the approach used for a device to be made aware of the characteristics of another device.

The IACL required at routing relays is different than that required at end system relays -- the concern is not with information usage. Information may be processed in some form at a routing relay but the result of this processing should not lead to an external action. To extend the idea of the IACL to these relays, characteristics of



concern possessed by these devices should be identified. The highest operational layer, at a routing device, is the layer of interest, although the same classifications of information routing characteristics may apply regardless of layer. A comparison similar to that between an IACL and device credentials would need to occur before protected information could be transferred. Possibly some of the other features made possible by the IPT, such as audit messages, would not be needed.

The IPT for a routing relay would need to be created along with the generation of the information to be protected. This is done at an end system. The IPT for a relay layer, would be submitted by the application layer as Interface Control Information and this would be passed down the protocol stack until it reaches the layer it is intended for. At that layer, it would be placed in a parameter as part of the protocol data unit. Currently available protocols may need to be updated to include an IPT parameter. This more generally can be called a routing parameter.

Devices operating at the application layer can also behave as routing relays as do those operating at the lower layers -- these devices are distinct from end system devices which also operate at the application layer. X.400 [12] describes entities called Message Transfer Agents (MTA) which receive, store, and forward messages along the path to the final recipient. MTAs have all seven layers of the OSI model and so act as relays at the application layer. The envelope contains information that directs the actions of the MTAs with fields such as originator's address, recipient's address, and priority. The envelope field message security label can be defined with ASN.1 to include an optional IPT which could direct the actions of the MTAs. The IPT as applied to any organized system of relay devices should be coordinated with the area of research called policy routing.

### 3.5.4 Encryption in the OSI Model

To practically apply encryption, it must be offered as a service at one or more of the OSI layers. Encryption of a PIU for data confidentiality can be effectively done in the presentation layer. But an interloper can conduct traffic analysis by tapping the address fields in a header. Traffic analysis involves obtaining the size and frequency of units of information sent from one party to another party. When setting up a connection-oriented channel, both the calling address and the called address are contained in the call request PDU. For a connectionless channel, both addresses are contained in the data unit PDU. One or more addresses are offered by each layer to the next higher layer as a way for the higher layer to access the services of the lower layer. Both source and destination addresses are generally present, either directly or indirectly through a channel code, in all the headers up to the highest layer contained in the PDU. Since addresses are contained in the headers of a PDU, the same techniques for protecting addresses are applicable to the other header fields.

A relay system that operates at the network layer, operates using the protocols at the physical, data link, and network layers. Encryption applied to the physical bit stream would protect all three layers. By separately encrypting the Transport Protocol Data Unit, that layer and all those above can only be accessed by the end users. The transport layer passes to the network layer the source and destination NSAP end user addresses. These fields when communicated between network relays can be secured through encryption but since the network devices will need to decipher the message to retrieve the address fields, for traffic analysis to be prevented the relays must be trustworthy.

With point to point links the intended recipient is clear. For a broadcast medium, whether on a LAN or a multipoint circuit, each device must watch the destination

address field for its address. An encryption scheme for a broadcast medium should include a means to avoid confusion caused by the decryption of a PDU by a non-intended recipient accidentally resulting in meaningful but incorrect information.

### 3.6 Attaching a Protection Tag to Protected Information

It was stated in Section 1.3.1:

In a limited environment, the policy governing which entities should have access to certain information, that is which designations should go into an access control list, is usually straight forward. This is because in a formal organization, decisions in general can be made by some position within an organizational hierarchy. In the everyday world the policy making governing this can be very complicated. In terms of private information generated in a transaction, many parties may be involved, each with self interests that may be in conflict with the self interests of others. How can this bargaining process be streamlined with technology so that the conduction of transactions is not hindered?

The first policy decisions are those concerning which information usage influences should be available for inclusion in information usage states. The decision to form a usage grouping is made centrally but for hierarchical groupings a usage influence is formed decentrally. Each entry in the Information Distribution Directory has an administrative body which decides upon the subordinate entries to follow it -- each creation of a subordinate entry results in the creation or identification of an associated administrative body.

The next policy decision is concerned with what information should be included in a PIU, which usage influences should be included in usage states, the control attribute values for each usage influence, and which usage states should be included in an IACL.

This decision is made through a negotiation process involving all parties involved in a transaction. Relative to the other parties, each party has a degree of bargaining strength. This is based on the overall desire of the other parties to complete a transaction. Information generated as a secondary outcome is just one aspect of a transaction; information generated as a proprietary product is a key aspect of a transaction. An end product of these negotiations -- the IPT -- is meant to control the actions of processing devices. This to some degree presupposes that to formulate the IPT in the practical world requires the use of processing devices and a strong interface between these devices.

### 3.6.1 Attachment Using the Processor Channel

In the past, the interface between processing systems belonging to each party to a transaction was often weak. For instance, a paper bridge may have connected mainframe computers belonging to different large companies involved in a transaction. For consumer transactions, the business party may have had a significant processing system whereas the consumer had none. The future promises to change this and presents the opportunity to effectively attach a protection tag to transaction generated information. In the future, at the time a transaction is conducted, while each party may (or may not) be communicating on a human level, each party will be represented by their own processing machine which will be communicating with the processing machines of the other parties. There will be many motivations for this machine interactive processing. Some of them will revolve around better record keeping and more efficient payment mechanisms. Among other steps carried out during the machine interactive processing can be the attachment of a protection tag to the information. At the simplest, the protection tag could have previously been determined, either through an active agreement process or by accepting default values, but a machine interactive bargaining process (possibly using artificial intelligence) may eventually be developed to reach, at

the time of the transaction or more likely sometime before, a protection tag agreeable to all parties.

In the past, processing power was fixed to a location -- terminal devices attached to telephone lines added some flexibility to the situation. When parties engaged in a transaction, particularly those offered to the public, the party manning the terminal had the advantage of controlling the informational aspects of the transaction. The smart card and portable radio-linked computers of the near future will provide the consumer with more control over a transaction. At the same time, the telecommunications linked computers used to conduct transactions between businesses will also afford more control over the generated information.

It will be assumed that a protection tag has been agreed to before a transaction is initiated. Therefore all parties should present the same protection tag. The main purpose of each party having access to its copy of the protection tag during a transaction is to allow all parties to confirm the accuracy of the protection tag before it is attached to the information to form a PIU. Also the information part of the PIU can be checked for accuracy and each party can have an exact copy of the PIU.

### **3.6.1.1 Smart Card**

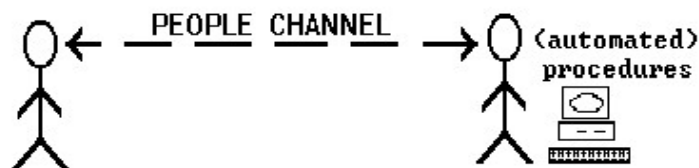
The smart card was suggested in Section 3.4.7.4 as a convenient way to carry around certificated personal usage influence tokens. The smart card should also become a popular approach for automating consumer-vendor transactions of which the needs of the protected information environment can be one concern. It can consist of just microprocessor and memory functions in a credit card-like case which is accessed by a terminal device, or a more sophisticated design may also include self-contained I/O functions. Since it operates without the need for its own telecommunications link -- its information storage and processing power are self contained -- it is not affected by the expense, absence or possible downtime of an interface to a telecommunications system.

The addition to the smart card of a personal radio link or a shared telecommunications interface at the vendor's terminal expands the resources of information reference, information storage, and processing power. All these resources can be centrally located or centrally coordinated which may be of particular advantage with information reference, or they can exist on the consumer's personal computer at home.

### **3.6.1.2 Integrated Services Digital Network**

For transactions at a distance all parties require a terminal device connected to the telecommunications system. ISDN from both a technical and a marketing perspective should create an effective link. ISDN can illustrate how dual channels can make it possible to attach a protection tag. One channel that exists, although in many cases it may not be needed, is the people channel. This is where a consumer presents a product to a cashier or where a person verbally engages in a transaction over the phone. The logistics of the situation, i.e., other customers waiting on line, preclude much discussion as to how the generated information should be handled. The other channel which exists to exchange detailed instructions on how to handle the transaction, is the processor channel. The basic-rate ISDN interface consists of two 64 kbps channels and one 16 kbps channel. While one of the 64 kbps channels can be used for the people (verbal) channel, either the other 64 kbps channel or the 16 kbps channel can be used for the processor channel. Since the voice signal is digital and can be processed using digital technology, the processor channel can be used to attach a protection tag to the voice information to form a PIU. The concept of dual transaction channels is illustrated in Figure 3.2.

### Single channel – Information processing inequality



### Dual channel – Information processing equality

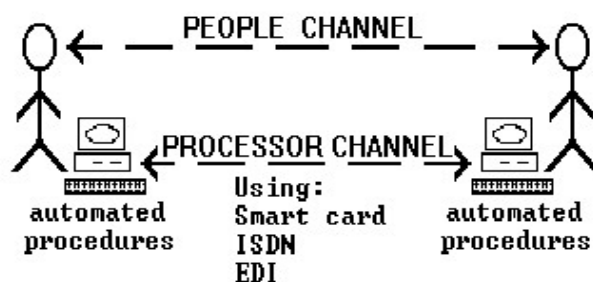


Figure 3.2 Dual channels aid with the conduction of transactions including the attachment of the protection tag to the generated information.

### 3.6.2 Devices Require Information Watchdog

The devices used by each party to effect both the processor and the people channels should be information watchdog resident devices, as is required to process protected information. In terms of the generation of the protection tag, the IPT is protected information except for those fields marked as nonconfidential items. When parties engage in a transaction, the information should first enter the information watchdog whether it is headed for a person or a processor. A smart card can securely make use of a terminal device to gain access to a telephone line (a convenient arrangement at a retail store), since all communications leaving the smart card's information watchdog can be encrypted.

### 3.6.3 Input Control Needs are Similar to those of Output Control

Procedures that bypass the exchange of information over the people channel should be illegal but many such bypass approaches, such as a clerk writing some information down on paper, does at least to some degree require an extra step for the information to enter the telecommunications system and thus be so easily reproducible and distributable. Information can leave the protected information environment from input as well as from output. The Device Type usage grouping and its control attributes which were discussed in Chapter 2 as a way to control output can be applicable to input. The IPT should be formed before the protected information section of the PIU is formed, and it can specify the type of input devices used by the other parties. This is only limited by the available secure I/O devices. Display devices are mechanisms for the output of information, and they aid with the input of information. Such devices can be designed to restrict the viewing of the images which they display. One possible way to accomplish this would be by combining retina scanning biometric technology with head mounted or eye glass display technology. Just as other usage groupings may be specified to restrict information distribution, a party to a transaction may want to be assured that the other originating parties possess certain usage influences before protected information is generated.

### 3.6.4 Connectionless and Connection-oriented Transactions

It has been assumed here that an agreement has been reached as to what the protection tag should be before the transaction is initiated. The way this is accomplished can depend on whether the transaction involves a connection-oriented relationship or a connectionless relationship. A connection-oriented transaction is formed by the parties meeting prior to the initiation of a transaction, to reach a mutually agreeable protection tag for each type of transaction that may be initiated. Generally this agreement will be



effective for a specified time period. Vendors usually have transaction procedures split between typical and atypical. The atypical procedures usually require a manager's approval or are conducted at a customer service desk or department -- this is where it makes most sense for the protection tag agreement process to occur. The processor channel can aid the agreement process by storing for easy access the user's IPT preferences.

For connectionless transactions, the parties have not spent time to reach a mutually agreeable protection tag before initiating the transaction. It is assumed that all of the parties would not feel it worthy to spend much time on agreeing to a tailored protection tag. In such cases the protection tag can be resolved in a number of ways:

- If all parties feel that the information to be generated does not need to be protected, then a protection tag should not be needed.
- If all parties have very limited aims for the distribution of the generated information (as verified by each party using the processor channel) then a simple protection tag can be formed at transaction time.
- The customer and vendor are both members of an intermediary organization such as a financial services company. The intermediary has previously worked out an agreement among its members as to what a protection tag should be for different types of transactions.
- The vendor uses an industry formulated standard protection tag and the customer is willing to use it as a default.

This last approach possess the possibility that the individual firms in an industry can conspire in a way contrary to anti-trust principles, in making a certain protection tag mandatory. Part of the bargaining power that a party to a transaction has in the formulation of the protection tag is that a party can forgo a transaction and enter into a similar transaction with other more amenable parties. Since the public doesn't read all

the fine print in a contract anyway, the prescribed use, usually by law, of a standard contract, has the advantage of protecting the public from unconscionable clauses. But now with the use of the processor channel, each party, in a sense, can read the fine print in milliseconds. A standard protection tag still has the advantage that the parties on the people channel do not need to process new information. The best of both worlds allows for a standard non-mandatory protection tag with regulatory oversight to see that it does not actually become the mandatory protection tag to do business in an industry.

## **CHAPTER 4**

### **THE INFORMATION WATCHDOG**

#### 4.1 Information Protection at a Device

When information is traveling between devices it can be protected from misappropriation through the use of encryption related techniques. At a device though, information must be in plaintext at some point so the processing can be based on the meaning of the information. Information protection at a device is concerned with internal threats and external threats. Internal threats make use of a device's (computer's) designed operation, external threats involve tampering with a device's and encompassing system's designed operation. This chapter addresses the need stated in Section 1.3.1:

In a limited environment, a certain degree of trust can be expected of all people who have administrative control over the physical security of a computer system. Assuming that the security system doesn't have any holes, the users can effectively be limited to permitted operations. In the everyday world, information may need to be sent to diverse computer systems for limited processing. The users may not be trusted to restrict their processing to the limited degree allowed. This problem can be solved by requiring in compliant processing devices a common security component controlled by the received information -- an information watchdog -- and by making it tamper proof.

The functioning of the information watchdog should prevent internal threats; its tamper proof construction should prevent external threats.

### 4.1.1 Internal Controls

The information watchdog is an internal control which adds features to the well known concept of the operating system kernel. To review, the security architecture of a computer is designed to accommodate the different degrees of trustworthiness of the programs that will run on it. The degree of trustworthiness of a program is used to allocate access rights to memory and the ability to execute specific instructions. This allocation of rights can be done on a hierarchical basis as shown by Figure 4.1. Moving in from the outside, each *protection ring* has new rights as well as all of the rights of the rings surrounding it. The kernel, in the center, can access all of memory and execute any instruction. A program in an outer ring can make use of the rights allocated to an inner ring but the use must be under the control of the inner ring. Therefore, each ring only has direct access to those rights to which it can be trusted. In a two ring system, the operating system would be in the center and the user programs would be in the outer ring. The operating system would protect itself from the user programs and maintain separations between user programs to protect them from each other.

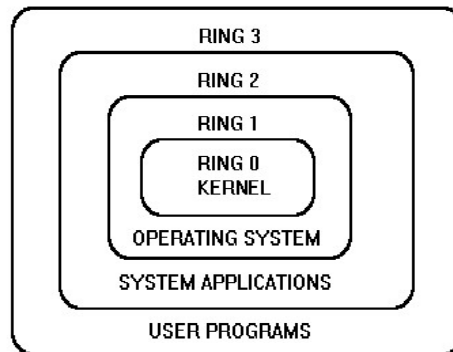


Figure 4.1 The Hierarchical Domain Architecture is based on the trustworthiness of groups of software

The information watchdog, in particular, implements internal controls by setting up boundaries between realized usage states in order to maintain the integrity of a PIU.

The information watchdog is not a separate ring but exists with the operating system kernel in the inner most ring -- the information watchdog just performs functions specific to the needs of PIUs. The information watchdog should be a standard component to help assure that it is properly produced. It presents a standard interface to other information watchdogs and to the rest of the operating system kernel.

#### **4.1.1.1 Protection Rings Related to Computer Aided Software Engineering**

The protection ring approach to keeping software honest can be related to another approach, Computer Aided Software Engineering (CASE), which can greatly help with the validation of the function performed by software as is needed for the Processing Function usage grouping. The protection ring approach is largely instruction based control. It determines which instructions can be executed, i.e., a write operation to a particular memory location. The operating system decides upon this in a dynamically changing environment.

A program's use of information occurs at a higher conceptual level than can be affected by instruction based control -- function based control is needed. It may be possible for a function audit to traverse the paths of manipulation performed on protected information but it may be very difficult without the right software tools. These tools operate in a static environment and can either perform a back-end role on completed software or can be involved during the generation of software. With CASE, functions should be able to be specified from which code can be generated. The concept of processing function is not necessarily correlated with processing function as identified by usage influences in the Processing Function usage grouping. Software validation would be greatly helped, though, if the functions that can be specified in a CASE system were in some way mapped to the usage influences. If the CASE product has itself been validated, and the functions programmed have purity, then the resulting code can be easily validated and assigned a certificated usage influence token.

#### 4.1.2 External Controls

External controls involving centrally controlled computers are fairly easy to implement. External controls, as described in Building a Secure Computer System by Morrie Gasser [16], involve:

- physical security,
- systems personnel security, and
- procedural security.

Physical security is concerned with such items as keeping the computer locked up behind closed doors. Systems personnel security is concerned with determining whom to trust with the development of systems software and with changes to the hardware. Procedural security is concerned with such items as the distribution of output from a computer. With a totally distributed system, as is the universal distributed non-trusted environment, a primary concern is with the external assault on the internal controls. In terms of the information watchdog, this assault could involve changing or gaining access to the secured encryption keys, or altering the functioning of the hardware.

#### 4.1.3 Current Systems at Risk

Various systems which carry information to the public are at risk of having their information misappropriated. The distinction between internal control and physical security external control will be shown for the information protection approaches developed for a few information systems:

- Cable TV.

Internal control -- A distorted signal is sent through the cable and a component located in proximity to an authorized receiver clarifies it.

Physical security external control -- The component is placed in a location which is difficult for an unauthorized person to access, possibly high up on a telephone pole or under lock and key.

- Digital Audio Tape.

Internal control -- Each DAT machine has a component which allows unlimited copies from an original tape but prohibits copies from a copy.

Physical security external control -- The component is an integral part of the circuit and tampering with it causes the equipment to malfunction.

- Computer Diskettes.

Internal control -- Various techniques exist to prevent copying of a diskette or to make copies ineffective. The latter can be accomplished with a dongle -- a hardware attachment to the parallel port which has a key that needs to match a key in the software.

Physical security external control -- The dongle could require specialized manufacturing and restricted distribution not freely available to the software consumer.

Procedural security external control does not exist in terms of administrative procedures at the end user, except to the extent that laws apply. For instance, it is illegal for a consumer to sell a copy made of a digital audio tape. Systems personnel security external control is of concern with the development of these systems and does not directly relate to the end user.

It is hoped that the information watchdog can supply a flexible common solution to information protection needs rather than application specific solutions such as those listed above. Due to the information watchdogs intended universal use, great emphasis must be placed on its external controls as is discussed in the next section.

## 4.2 External Controls for Watchdog Resident Devices

The external controls for an information watchdog resident device are designed to accommodate the device to the non-trusted environment in which it is situated. The external controls must in a sense be internalized or further systematized. In some cases external controls are placed within the information watchdog which primarily provides for internal control. The external controls mentioned in the preceding section are implemented for information watchdog resident devices in the following ways:

- Physical security is designed into the construction of IW resident devices. It must not be able to be bypassed so that internal controls are compromised.
- Systems personnel security is accomplished by only allowing select design and manufacturing teams to be involved with the creation of an IW. The design and manufacture of the rest of an IW resident device, must be closely watched by an independent auditor. Usage states at a device must be validated in an independent manner.
- Procedural security is managed by allowing an originator of information to have great specificity in the restrictions that can be placed on the output of information from the protected information environment.

### 4.2.1 A Design for Built-in Physical Security

There are a few basic physical attacks which can be perpetrated against an IW protected device in order to fraudulently gain access to information -- expose a point of plaintext data flow, extract the private key, extract a secret key, or alter the code within the kernel of the operating system.

First, the installation of a private key into a device must be a secure process. When the private key is placed in a device, its corresponding public key is certificated by a trustworthy process overseen by an independent trustworthy administrative



organization. The certification, among other things, indicates to the public that the private key has securely been inserted into the device. The entire manufacturing process of an IW protected device must be highly controlled and the insertion of the IW, with its private key, into the device is a crucial aspect of the manufacturing process. It is envisioned that highly automated manufacturing techniques will make practical the needed level of control. Therefore, the user of an IW protected device is in the same position as any potential eavesdropper along the transmission path. (As mentioned in Section 4.3.2, during manufacture a private code rather than the actual private key may initially be installed in a device.)

In addition to the secure installation of a private key, it must not be able to be extracted. There may be a technique to hide the private key information on a chip. This can be related to the desire of chip manufacturers to make reverse engineering more difficult. Although a hiding approach may be largely successful, I believe that hiding is probably harder to accomplish than destroying. The entire IW protected device can be designed to have its functioning disabled (destroyed) upon tampering, including the code repository of the IW. For instance, if the repository could be constructed with programmable fuses and if a small reliable internal power source was available then any attempt at tampering could cause all of the fuses to be blown thus erasing the codes [17, p. 748]. Alternatively, the state of the code repository or the state of the entire device could require steady power for its maintenance. Any significant physical invasion could in essence require the perpetrator to make an incision of the device's "circuit" resulting in an open condition and the cut-off of power flow. The state of the device would then be lost or erased including the private key and any plaintext.

Instead of using a passive approach where the act of an intruder directly results in the loss of power, an active approach may be more easily implemented. The outer casing of an information watchdog protected device could be monitored for its

resistivity. A standard value could be predetermined for each device design. The resistivity monitor would constantly compare the measured resistivity with the preprogrammed standard value. A significant variation from the standard would result in a signal for the power supply to turn itself off. Thus any attempt by an intruder to separate the casing or to cut a hole in it would disturb its resistivity resulting in the loss of the state of the device.

In addition to the outer casing, an inner casing is also needed. Electromagnetic radiation should be prevented from leaving the device so that the plaintext contained within it is not revealed, and electromagnetic radiation should be prevented from entering the device so that the operation of the device is not altered.

#### 4.2.2 Compliant Devices and Modularity

As mentioned in the introductory chapter, an information watchdog must be resident in each compliant device. A device, in turn, is any item of processing equipment which in all cases can be directed in its processing of protected information by a single (or unified) information watchdog.

It was mentioned in the previous section that all physical access to the circuitry of an IW protected device is prohibited so that plaintext is not exposed and so that the functioning of the device is not altered. This precludes the ability to repair broken devices or to allow uncontrolled customization of a device. But a certain level of modularity can be achieved in order to change broken parts or to alter functionality in the field. This is accomplished by making each module a compliant device with its own IW and private key. Of course, doing so can involve greater cost and diminished performance, and so a trade-off exists between modularity and performance.

### 4.2.3 System Survival in a Compromised Device Environment

#### **4.2.3.1 Limited Time Periods for Device Key Pairs to Force Security Inspections and Updates**

The time period of validity can help control the problem that would result from a successful breach in the built-in physical security of a device. Ideally a device would be tamper proof and this would allow for its key pair to be active for an unbounded duration without intervention from the CA or a delegate of the CA. Since the threat of successful tampering will always exist, a limit on the time period of validity would force an owner of a device, at expiration time, to have the built-in security of a device validated. This process can be thought of analogously to the annual safety inspection that is performed on an automobile. The benefit of a program of security inspections would need to outweigh the cost. The cost and reliability of the inspection can be favorably impacted by designing a device for automated test procedures.

An extension of this idea could use the time period of validity to cause the expiration of a device, rather than just the device's key pair. Devices could then be replaced with updated devices with new built-in security features to counter the new threats perceived during the prior time period of validity. Of course, this would be a costly requirement but it is possible that the additional protection it offers private and proprietary information would justify the cost.

As explained in the following section concerned with logical built-in security, it may be possible to perform a type of encryption on information which resides within a device. Only at arithmetic and logic points would the plaintext need to exist. Therefore, only the arithmetic-logic unit (ALU) would need to be secure thus requiring a periodic update of only the ALU. This would substantially reduce the cost of a program of forced periodic device replacement.

#### 4.2.3.2 Logical Built-in Security

The transport of information within space (transfer) and time (storage) is suitable for encryption since the transport function is not based on the meaning of information. At a device during processing, the meaning of information is required when doing arithmetical and logical operations. Usually processing involves intermediate results which are temporarily stored within registers and memory for rapid retrieval. It should be feasible for encryption to be performed on the temporarily stored intermediate results, as well as on the software code loaded into memory. The following sketches some of the ideas as to how this may be done.

The encryption unit could either use a few secret keys which are randomly allotted to memory locations via an assignment function, or a separate secret key could be assigned to each memory location via a random key generator function:  $secret\_key = f(random\_number, location)$ .

The robustness of an encryption scheme depends on the number of possibilities with which plaintext can be represented. For the sake of efficiency, a read or write memory access of encrypted data should not require multiple bus accesses. With encryption for a byte there are only  $2^8=256$  possibilities; with encryption for a 32 bit word there are 4.3 billion possibilities. Clearly the wider the bus, the more effectively can encryption be implemented. The encryption scheme must protect against a known plaintext attack. Since a memory location can be repeatedly written to, a pattern can be formed which could either help to reveal the encryption key or generate a code book with which to decode the information. Therefore, an encryption key would need to be periodically changed. The rate of change could depend on the number of writes performed or the length of time in use. If the above function is used to assign secret keys then the random number would need to change periodically. A change in a secret key would require an encryption update of the data sitting in memory.

Another level of protection would be achieved if during the update process, the locations of data items were changed. This could be based on a location generator function:  $location\_absolute = f(random\_number, location\_relative)$ , where the random number would periodically be changed. While the location switch is made, the data would need to be buffered within the encryption unit so that its path of movement would not be obvious. Re-encryption and location switch could be performed during bus cycles which are not occupied with ALU work. If the ALU's use of the bus is constant then the encryption unit's use of the bus would need to take precedence.

Plaintext would now only be available to the ALU and the encryption unit. The remaining items which must be kept secure are the private key, the public key of the CA, the kernel of the operating system, and the secret keys for storage, memory, and registers. All of these items could comprise an expanded definition of an information watchdog. The information watchdog would need to exist within a secure chassis but the remainder of a device would not. This would greatly reduce the cost of forced periodic replacements of devices. Such a requirement would be needed to refresh the installed base of information processing equipment with safeguards against the latest perceived physical threats.

For output devices, there is usually a component which converts digital information into a signal which can drive the output mechanism. A conversion unit would also need to be secure since its input is plaintext but the above scheme does not protect the channel carrying the drive signal to the output mechanism, nor does it protect the output mechanism. It can be argued that once information is allowed to be displayed to the degree that it leaves the Protected Information Environment, the protection of information is not controllable anyway.

#### **4.2.3.3 Opportunity for Information Compromise Based on Type of Information**

The generators of private information generally prefer that its distribution be limited. The selection of the information usage influences of Person, Administration, and Device ID can add the element of trust to an information usage state. Therefore private information can be directed to only those parties which are trusted to do the right thing. Since usage influences are validated by trustworthy independent agencies, the receipt of protected information by only selected parties can reasonably be assured.

The generators of proprietary information generally prefer that its distribution be wide. This is because each information transfer can be a sales transaction. The wide distribution of proprietary information may justify another application of the digital signature as is described in the next section.

#### **4.2.3.4 Control over Re-entry of Fraudulently Extracted Information**

The built-in security described to this point, if circumvented, would allow for protected information to leave the Protected Information Environment. In some instances, particularly those involving a technological conversion from digital code to output, the usefulness of information is dependent on the acceptance of the information by the required output device. Where similar output devices are available, some for the PIE, and others for use outside of the PIE, fraudulently extracted and copied information can be processed by the devices outside of the PIE.

If the manufacturers of a type of device or the manufacturers of key components of a device can all agree (possibly with the help of international law) to manufacture for the PIE, then the protected information can be coded so that non-allowed copies will not be accepted by the required output device. What determines the allowed flow of information are the usage states within an IACL. For each type of device (particularly output devices) to which information is directed, for instance, a digital music player, the PIU can be digitally signed by the designated device authority for that particular type of

device. The signature, similar to that which is performed by an information originator (see Section 3.3.2) is applied to a hash result of protected information and IACL. Therefore the integrity of the PIU can be maintained. That is, a valid IACL can not be stripped off from the information and replaced with a fraudulent IACL. The PIE compliant device would check the validity of the information's device signature and would then determine if based on the usage states within the IACL, it is allowed read access to the information. The fraudulently copied information would then only be of use if counterfeit devices could be manufactured. The controlled distribution of key components would be one impediment to such an operation.

#### **4.2.3.5 A More Modest Goal for Built-in Security**

The question still remains as to whether and to what degree the requirement for built-in security can be met. In any case, the expectations of the system users must match the reality of the effectiveness of the design. Different levels of effectiveness can satisfy different needs. At the extreme level of bypass prevention ineffectiveness, the information watchdog would simply be a voluntary aid for the immediate user in carrying out the directions in the information protection tag. The information watchdog, in this situation, can be a typical add-in board. Pressure to follow the directions in the information protection tag may still come from law or intra-organizational rules.

### 4.3 Internal Controls for Watchdog Resident Devices -- The General Purpose Computer

Processing machines come in many architectures and the future probably has in store new variations and new approaches. The internal functioning of IWs can vary to suit the needs of particular architectures but to facilitate their proper design and construction, each IW variation should be a standard component.

One common processing machine architecture is the general purpose single CPU multiple I/O processor computer. Such machines consist of a number of resources

which are managed by an operating system. (This approach to thinking about operating systems is based on Operating Systems by Madnick and Donovan [8]). The resources are grouped into four categories -- information, device, memory, and processor. The four resources of the operating system are diagrammed in Figure 4.2.

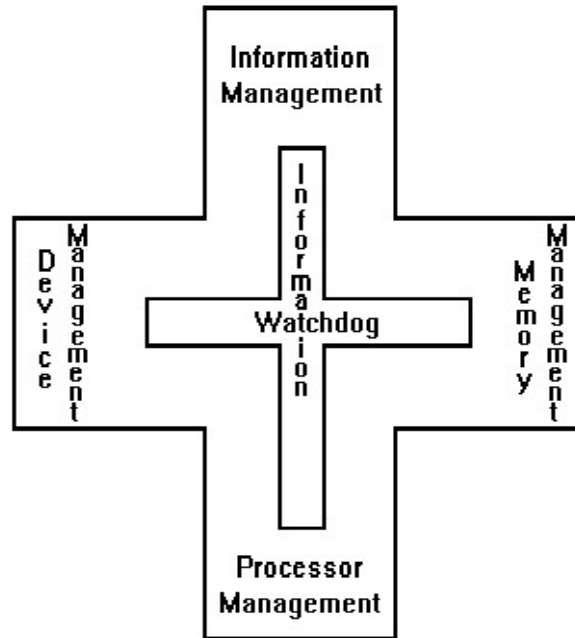


Figure 4.2 The Information Watchdog is implemented within the four resource managers of an operating system.

Madnick and Donovan [8, p. 8] state, "Viewing the operating system as a resource manager, each manager must do the following:

- Keep track of the resources.
- Enforce policy that determines who gets what, when, and how much.
- Allocate the resource.
- Reclaim the resource."



In the protected information environment, each of these functions must be carried out for the four resources so that the instructions contained in an IPT are adhered to. Many of the same functions that can apply to managing non-PIUs can as well apply to PIUs -- the functions specifically implemented to handle PIUs are considered part of the information watchdog. Since this paper is concerned with controlling access to information, the following sections which describe the four resources as managed by the information watchdog will emphasize the "who gets what" function, as phrased in the following questions:

- Information Management: Can a PIU be written to another PIU?
- Device Management: Can a PIU be transferred to another device?
- Memory Management: Can a PIU be placed in specific memory areas?
- Processor Management: Can a PIU be accessed by an application?

#### 4.3.1 Information Management

Information at its fundamental level consists of bits. These bits are formed into data structures such as octets, fields, records, and files. All data structures exist in the protected information environment, but whatever data structure is selected for protection must have an IPT logically associated with it. Protected information unit (PIU) is the general term that has been used for a protected instance of data. The prefix "protected information" can apply to any data structure. For data structures constructed of other data structures, a decision must be made as to what level to apply the IPT -- generally it will apply to the top level of construction and the PIU will consist of all the data. The following are the information management functions of the information watchdog (IW), arranged in the approximate order in which they would be performed:

- The IPT must be accessible to the IW as a data structure -- the IW must be able to strip off the IPT from the rest of the PIU and be able to interpret its fields.

- The IW must make a copy of the nonconfidential items in an IPT and associate it with the PIU through a code. The copy must be non-IW-protected.
- Upon opening PIUs for read access, the IW computes the combined IACL. All PIUs that are to be processed at the same time must be opened for reading at the same time -- the codes specifying the PIUs can be included as parameters in a single instruction. The combining of the individual IACLs can be done with a Boolean AND operation as was discussed in Section 2.1.2.3. Of the control attribute values specified for a usage influence which the device is validated for, the most restrictive value (as specified in the IDD and stored at the device) must be selected. The combined IACL is called the least common IACL (LC IACL).
- The IW determines if the usage state of the current application (as placed in the Usage State Table by processor management) satisfies the LC IACL. This is done by evaluating the Boolean expression of the LC IACL where a variable is TRUE if it exists as a validated usage influence in the Usage State Table. If it is satisfied, the LC IACL is stored in the LC IACL Table and this and the individual PIUs are made available to the application for read access. An application may open a PIU for read access just to read the IACL or the originator's link section of an IPT. Branching logic may be based on these fields.
- As discussed under memory management, an area of memory, called a Protected Information Memory Area (PIMA) is specified when PIUs are opened for reading. The LC IACL controls read/write access to the PIMA. This memory generally serves as a work space but particular addresses can serve as data ports to various hardware functions. As discussed in Section 3.4.7.2, these hardware functions at a device are officially identified as Device Type usage influences and their memory assignments are entered into certificated tokens. At boot up these memory assignments are loaded (by processor management) into the

Device Type Memory Map Table (DTMMT). Information management after computing the LC IACL checks the DTMMT to see that all of the Device Type usage influences associated with the addresses in the active PIMA are included in the LC IACL. Each memory address of the PIMA can be thought of as a separate recipient of the protected information. In a sense, the Boolean expression of the LC IACL can be satisfied for each memory address. The PIMA is opened in total though, so for the open command to be carried out, all of the addresses in the PIMA must satisfy the LC IACL.

- Before opening a PIU for write access, the IW determines if its IACL is as or more restrictive than the LC IACL. An approach to do this using set theory was demonstrated in Section 2.1.2.

The instruction for opening a PIU for write access can have a parameter to request that the LC IACL be used for the PIU's IACL.

"Writes" involving memory mapped I/O can only be done to non-reconfigurable memory or storage. "Sends" to other (information watchdog resident) devices are performed by device management.

- A PIU update access can be allowed by the general operating system but it must be handled by the information watchdog as a read and a write in terms of access control. For delete access, a PIU creates no special requirements, other than to delete all the remnants of the PIU found in special files and tables.

#### 4.3.2 Device Management

Device management is concerned with the transfer and storage of information. The IW in particular is concerned with the transfer of a PIU to another IW resident device and with the transfer of IPT protected information to storage or to nonvolatile memory. The following device management functions of the IW can be related to an internal operation, an outgoing PIU, or an incoming PIU:

#### 4.3.2.1 Internal Operations

- For "writes"/"reads" from nonvolatile memory or storage, a seamless encryption/decryption is performed. Public key cryptography is not mandated here and probably a faster scheme should be used. The nonvolatile nature of the memory/storage requires encryption in case this subassembly is dislodged and removed.
- The IW self-generates a private/public key pair. The private key is never revealed outside of the information watchdog. This function needs to be done once, but some unforeseen advantages may exist if this function can be done on demand. Before the public key can generally be used, it must be certificated by being included in a certificate of the type shown in Section 3.4.2. A symmetric key also needs to be self-generated. A symmetric key is used to encrypt information for transfer to nonvolatile memory or storage and for the receipt of a PIU from another IW resident device. A symmetric key can only be used once (or must be limited to two specific devices) for transfers of PIUs between IW resident devices, since the ability to encrypt is the ability to decipher other PIUs headed for a receiving device.

A method is needed to authenticate to the certification authority the relationship of the public key to the device ID. The method can rely on a private device ID which uniquely corresponds to the public device ID. If only the individual information watchdog and the certification authority has this information, the relationship of public key to public device ID is authenticated.

#### **4.3.2.2 Outgoing PIUs**

- Accept requests for the transfer of PIUs from application programs at the device ("send" command). Other devices can request that a PIU be sent to it but this communication is done with application programs at the sending device using nonconfidential identifying information.
- Ask for DATs from potential receiving devices and decipher them.
- Compare device credentials in a received DAT to the IACL of the PIU requested to be transferred. If the IACL is satisfied and the transfer is allowed by a table of administrative directives then the PIU can be sent.
- Send audit message to requesting originators.
- For data confidentiality, encrypt outgoing PIUs, and audit messages with the receiving device's public key, or in the case of outgoing PIUs, with a symmetric key, if supplied. For data integrity, sign PIUs and audit messages with the sending device's private key.

#### **4.3.2.3 Incoming PIUs**

- Send DATs to requesting devices as long as the transfer of the DAT is allowed by a table of administrative directives. A DAT is encrypted with both the private key of the receiving device and with the public key of the potential sending device.
- Decipher incoming PIUs with its private key or with a symmetric key, if it was supplied to the sending device.
- Notify applications of received PIUs. PIUs will be sent (by the sending device) to a PSAP address -- the port to an application. An application may not be able to access the PIU based on an IACL conflict but it may be permitted, by the general operating system, to access the PIU's nonconfidential items.

### 4.3.3 Memory Management

The memory management function in general is concerned with the allocation and deallocation of the memory that processors directly access for instructions and data. Since the memory may be shared by a number of tasks or programs that may access PIUs with different LC IACLs, the memory management function must see to it that a given allocated memory space, at any instant, only stores data to which the same LC IACL applies. Such a memory space will be called a Protected Information Memory Area (PIMA). Over time different LC IACLs can be assigned to the same PIMA.

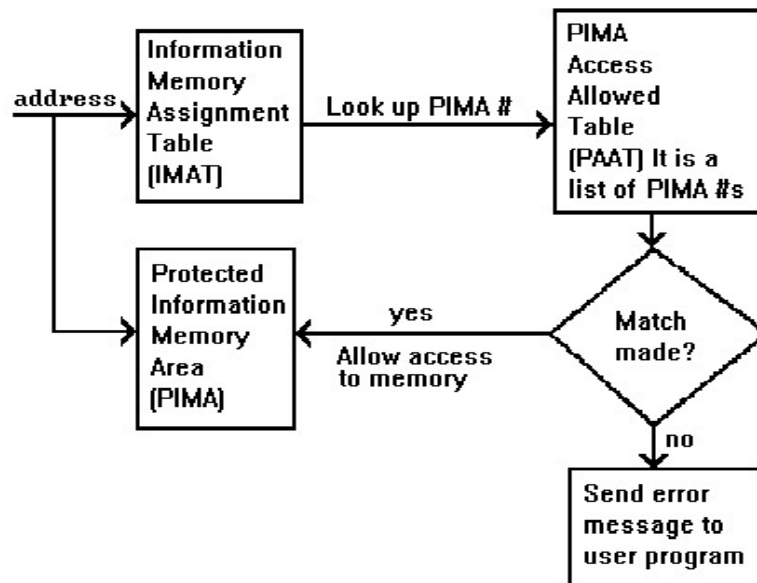


Figure 4.3 Protected Information Memory Access

The Protected Information Memory Area (PIMA) is reserved in an assembly language program in typical fashion by directing the assembler to reserve for the program sections of memory. A directive command is needed which will allow the

programmer to assign a data section to a PIMA. The output of the assembly will be a file containing the machine language program and a table of the assignments of data sections to PIMAs. This is called the Information Memory Assignment Table (IMAT). At execution time, memory management will load the IMAT in memory. Every access of memory will make reference to this table, so the table should be sorted by memory address with the table look up result being the PIMA code. A hardware implementation could speed up this reference. The check done on each memory access is shown in Figure 4.3. Also verified but not shown in this diagram is whether the access granted is for reading only, or for reading and writing.

A typical user program may need to access PIUs which have conflicting IACLs. This is a situation that the programmer and/or the user of the program need to be fully aware of, since they must explicitly request protected information related context switches in the program. When the program requests such a context switch by selecting a PIMA and opening one or more PIUs with IACLs which can result in a LC IACL, memory management conducts the following actions:

- a. Records user accessible register values in a storage area for the previously active PIMA. This area is called the PIMA Context Storage Table.
- b. Records the entry in the LC IACL Table in the PIMA Context Storage Table.
- c. Places the newly selected PIMA identifier code in the first entry of the PIMA Access Allowed Table (PAAT). During memory accesses by the user program, the PIMA corresponding to accessed data sections must be found in this table.
- d. Has information management formulate the new LC IACL based on the PIUs opened. This is placed in the LC IACL Table. The steps so far are shown in Figure 4.4.
- e. Compares the entry in the LC IACL Table with the LC IACL stored in the PIMA Context Storage Table for the active PIMA. If the active LC IACL is as or more

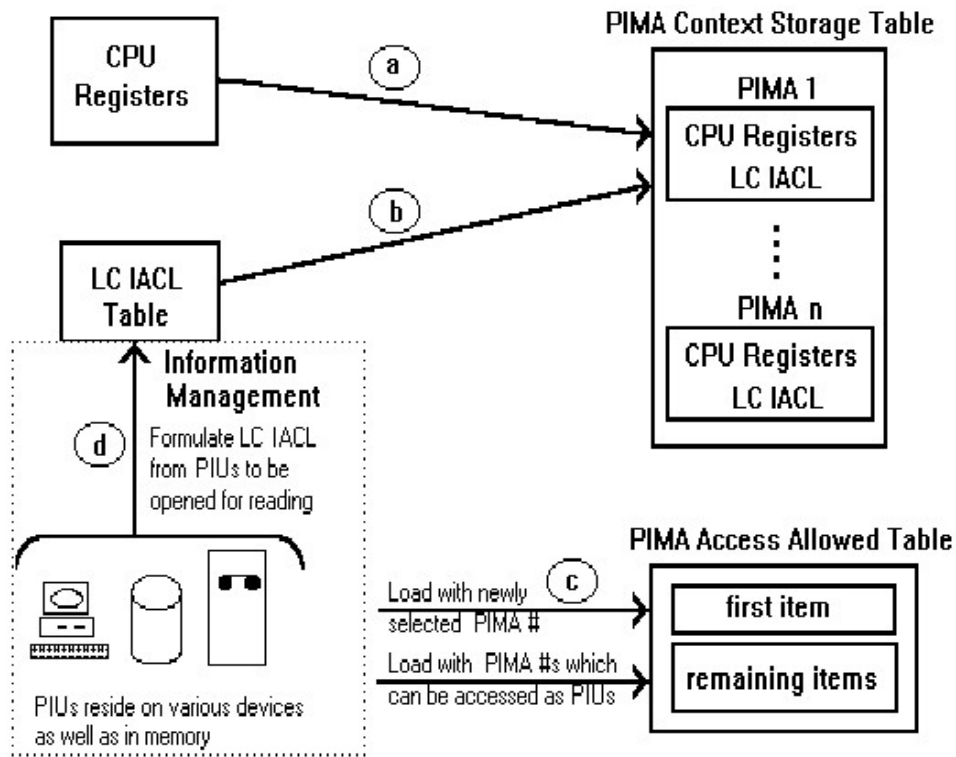


Figure 4.4 Memory Management: 1st Phase of Context Switch

restrictive than the previous LC IACL for the active PIMA then the stored register values for the active PIMA are copied into the registers. If the active LC IACL is less restrictive than the previous LC IACL then the user accessible registers and the PIMA (memory) are set to a value of zero. This last step is shown in Figure 4.5. This approach allows processing which makes use of a single LC IACL to continue undisturbed through a series of context switches. On the other hand, this approach also allows an area of memory and the variables defined for it to be reused by processing which accesses PUIs with various IACLs.



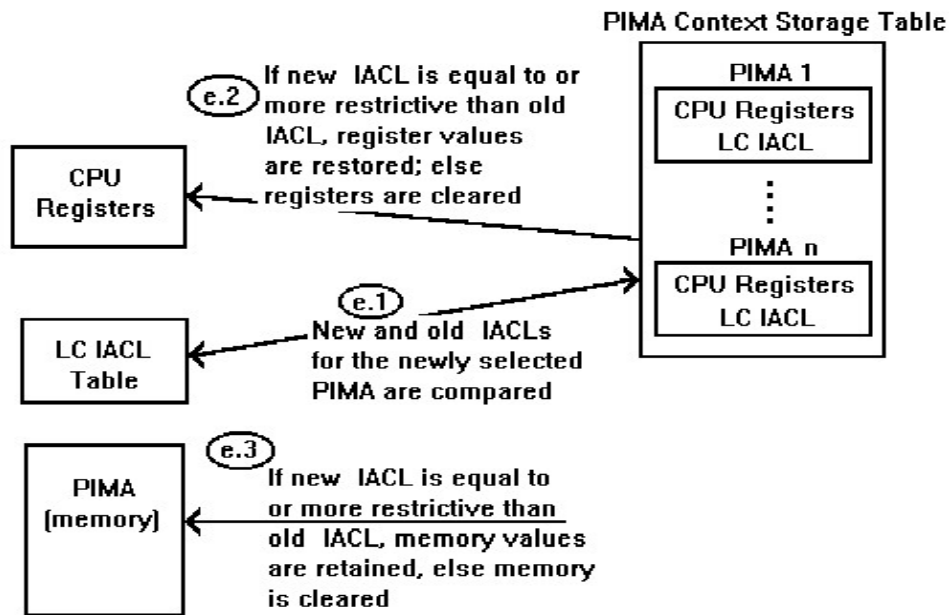


Figure 4.5 Memory Management: 2<sup>nd</sup> Phase of Context Switch

When a PIMA is no longer active, the data stored in its memory and its IACL are still available. Information and a corresponding IACL are the two main ingredients for a PIU. Therefore an inactive PIMA can be treated as a PIU when information management opens PIUs for reading. To allow access to these PIMAs, their identifiers must be included in the PIMA Access Allowed Table.

#### 4.3.3.1 Example of Memory Management (and Information Management)

An example of how a user program can be organized to make use of the PIMAs, could involve a simple hypothetical credit card billing program at a retailer. The program reads in credit card sales transactions in the order in which the sales were made. The retailer accepts credit cards administered by Credit Card Companies 1, 2, and 3. The program in essence first checks the validity of the credit card number to make sure that a stolen card has not managed to bypass the initial control procedure. Then it allocates sales transactions to credit card company and computes the total sales charged

to each credit card company as well as the total of all credit sales transactions for the retailer. This is illustrated in Figure 4.6.

		Key: R=Retailer,			
		B <sub>x</sub> =Business,			
		C=Credit Card Issuer,		IACL	PIMA
		S <sub>x</sub> =Shopper		-----	----
Credit Card Company 1					
Shopper 1	\$ xx.xx	R;	B <sub>1</sub> , C;	S <sub>1</sub>	I
Shopper 3	xx.xx	R;	B <sub>1</sub> , C;	S <sub>3</sub>	I
Shopper 3	xx.xx	R;	B <sub>1</sub> , C;	S <sub>3</sub>	I
Shopper 5	xx.xx	R;	B <sub>1</sub> , C;	S <sub>5</sub>	I
-----					
Total	\$ xxx.xx	R;	B <sub>1</sub> , C		II
Credit Card Company 2					
Shopper 2	\$ xx.xx	R;	B <sub>2</sub> , C;	S <sub>2</sub>	I
Shopper 3	xx.xx	R;	B <sub>2</sub> , C;	S <sub>3</sub>	I
Shopper 7	xx.xx	R;	B <sub>2</sub> , C;	S <sub>7</sub>	I
Shopper 8	xx.xx	R;	B <sub>2</sub> , C;	S <sub>8</sub>	I
-----					
Total	\$ xxx.xx	R;	B <sub>2</sub> , C		III
Credit Card Company 3					
Shopper 5	\$ xx.xx	R;	B <sub>3</sub> , C;	S <sub>5</sub>	I
Shopper 5	xx.xx	R;	B <sub>3</sub> , C;	S <sub>5</sub>	I
-----					
Total	\$ xxx.xx	R;	B <sub>3</sub> , C		IV
=====					
Grand Total	\$ xxx.xx	R			V

Figure 4.6. Example of Memory Management

The initial sales transaction in Figure 4.6 has an IACL with three information usage states. This IACL can be expressed with the Boolean expression:

$$(\text{Administration} = \text{Retailer}) + (\text{Administration} = \text{Business}_x)(\text{Line of Business} = \text{Credit Card Issuer}) + (\text{Person} = \text{Shopper}_x)$$

Omitting the explicit specification of the usage groupings and using the abbreviations in the Key of Figure 4.6, the Boolean expression can be expressed as  $R+B_xC+S_x$ .

The input to the application program is a file consisting of sales transaction records, where each record is a PIU (a protected information record, to be specific). The output is a number of protected information files -- a separate file for each shopper containing all of the sales transactions for that shopper, a separate file for each credit card company containing all of the sales transacted using a credit card issued by that company and including a dollar total, and a file for the retailer containing all the information in all of the credit card company files and including a grand dollar total.

A general rule which directly applies is that as more PIUs with diverse IACLs are aggregated, the more restrictive is the combined IACL. The IACL for the file for Credit Card Company<sub>1</sub> is  $(R+B_1C+S_1) (R+B_1C+S_3) (R+B_1C+S_5) = R+B_1C+S_1S_3S_5 = R+B_1C$  since as per Section 2.1,  $S_1, S_3,$  and  $S_5$  are mutually exclusive. The IACL for the file for the retailer is  $(R+B_1C) (R+B_2C) (R+B_3C) = R+B_1B_2B_3C = R$ , since  $B_1, B_2,$  and  $B_3$  are mutually exclusive. Processing would proceed as follows:

a. The first PIU of a credit sales transaction is opened for reading. The open command has a parameter which specifies that PIMA I is to be the work space in memory for processing the opened PIU. (A work space can be read from and written to.) The IW computes the LC IACL which is the IACL of the PIU credit sales transaction since it is the only PIU opened. The LC IACL automatically applies to the work space PIMA.

Using PIMA I as work space, the validity of the charge account is determined. The customer's protected information file is opened for writing and a record is written, the contents of which, depend on the outcome of the validity check. This information must be written to a PIU that has an IACL which includes the shopper's usage influence (a separate PIU for each shopper). Otherwise, the shopper could not be contacted if there is a problem. Since PIMA I does not need to retain its information, it can be reused for the processing of each sales transaction -- the context switch, before each sales

transaction's protected information record is opened, clears the allocated memory area and registers.

b. The sales transaction now needs to be included in the appropriate credit card company's file. This information is still available in the opened protected information record or in PIMA I, and based on the IACL obtained from either place, the application program can determine which credit card company's PIMA should be opened. In Figure 4.6, Company 1 has PIMA II, Company 2 has PIMA III, and Company 3 has PIMA IV.

Once a read open command is given, the previously opened PIUs and PIMAs are closed. The read open command must specify either the credit sales transaction's protected information record or its PIMA so that the input data can be accessed. Since the PIMA also includes the results of the validity check, it is the better choice. When a PIMA is opened for read access, the IW puts the PIMA's identifying code in the PIMA Access Allowed Table.

The PIMA work space for a credit card company's information, needs to remain in place as different credit sales transactions are processed (alternatively, the data could be written out to a PIU and then read in each time as needed). Therefore, its IACL must not contain a usage state for a shopper. This is done by shaping the LC IACL by including the IACL of the PIU that will eventually be opened to hold the results in the credit card company's PIMA, or by directly assigning the required IACL to the PIMA. The LC IACL of  $R+B_xC$  becomes the IACL of the current work space PIMA.

c. To compute the grand total, an open for reading statement can include all the PIMAs for the credit card companies in conjunction with the opening of the retailer's PIU for both reading and writing. The active LC IACL would just include the retailer, R, and the computations would all occur in PIMA V.

This example has made use of most of the IW features concerning memory: PIMAs which are used with different IACLs, user program branching based on the IACL of a PIU, PIMAs which retain their data since they are used with a single IACL, and PIMAs which are treated as PIUs so that their data can be accessed by another PIMA.

#### **4.3.3.2 Memory Allocation in a High Level Language**

Just as data sections in an assembly language program which will hold protected information must be assigned to PIMAs, variables in a high level language must also be assigned to PIMAs. An analogy can be made to the different types of variables local to a function in the language C. In C, static variables retain their values between function invocations, whereas automatic variables do not. Variables assigned to PIMAs which do not have changing IACLs, behave as static variables in relation to protected information related context switches. A changing IACL for a PIMA, results in automatic variable behavior. Therefore variables local to a function can be either static or automatic in relation to function invocations, and static or automatic in relation to protected information context switches. This two dimensional aspect of variables must be taken into account when programming.

#### **4.3.4 Processor Management**

The processor management function is generally concerned with the allocation of the processor to different tasks and programs. This can involve multitasking and multiprogramming or simply be the dedicated allocation of the processor to the next on a queue of programs. For protected information considerations, the main issue is whether or not a particular task or program is allowed to access a given PIU. Just as information, device, and memory management determine respectively if a PIU can be

transferred to another PIU, to a device, or to a section of memory; processor management determines if a particular application can access the information.

A single computer could conceivably have a diverse variety of application programs running on it or a renegade programmer could write a program to extract protected information from a computer. Therefore, the usage state associated with an application must be determined and compared with the IACL of a PIU before the application is allowed to access the PIU.

Processor management involves the gathering of validated usage influences. These are fed to device management which forms the device credentials, and those usage influences associated with the application to which the CPU is about to be allocated, are entered into the Usage State Table. The Usage State Table is referenced by information management when determining if the current state of a device satisfies the LC IACL.

The condition of a usage influence must be determined on a timely basis. In terms of hierarchical groupings, condition means presence or absence; in terms of continuous groupings, condition means parameter value. The utmost in respect to a timely basis would be an update of all usage influences immediately before all transfers of DATs and all context switches involving a change in application. Both operations may be done at such a high rate that the condition of a usage influence can be considered to be static. Since an update of a usage influence can use resources and take time (the Location grouping of usage influences, for instance), rules, simple as well as algorithmic, should be developed to determine when a usage influence should be updated.

Based on these rules, an update period should be specified by the validating authority when a usage influence is being validated. Each certificated token has a period of validity during which the accompanying usage influence can be treated as valid. The method used to determine this period of time is developed by the administrative body

identified in the corresponding entry of the Information Distribution Directory (see Section 2.4.3). The resulting time period should match the period of time when the usage influence is actually valid, although the accuracy of this estimate may vary. Where a human procedure is needed to validate a usage influence, for instance, personal usage influences, processor management must alert the user of the impending expiration; where the procedure is automated, processor management must initiate the renewal process. The determination of which usage influences should be validated and gathered by processor management should be based on a table of locally specified administrative directives.

#### 4.3.5 Recap of Changes Needed to Systems Software

In order to implement the proposed information protection enhancements, certain changes will need to be made to existing systems software. The ideal situation is for these changes to leave the systems and their applications upward compatible. This allows all existing software which is not involved with protected information to still be executable. It is also hoped that the needed updates will be relatively easy to implement. The following changes will need to be made to systems software:

- An existing operating system will need to be rewritten to include the information watchdog. (The IW will need to be, at least partially, a hardware component so that it can hold the primary signature information.) The IW should be a standard component and so an operating system will need to be rewritten to, at a minimum, interface with the IW and with application programs.
- The high level language will not need to change although certain functions for opening PIUs, reading IPTs, and sending PIUs will need to be written by systems programmers. It will then be necessary for an application program to invoke these functions when opening PIUs for reading or writing.

- An applications program will need to assign variables to PIMAs and a preprocessor that is executed before compilation should aggregate these variables per PIMA and present them to the compiler as contiguous segments or buffer areas.
- The use of a multitasking executive complicates protected information related context switching since the channels and signals between tasks which are made available by the multitasking executive is another path for the distribution of protected information and so must be controlled. This requires that the LC IACL always accompany the message so that if a protected information related context switch occurs while the message is sitting in a channel, the executive can determine by comparing the old and new LC IACLs if the destination task can receive the message.
- Related to the issue of multitasking channels is the issue of covert channels which may be created by various systems software. As explained in Building a Secure Computer System by Morrie Gasser [16], there are two basic types of covert channels -- storage and timing. A storage channel occurs when one user program can write an object which can be read by another user program. An example of this is the ability of programs to create and name files, with the file names being readable by other programs. A timing channel occurs when one user program can cause an event to happen at a variable frequency that is somewhat controllable. An example of this is the ability of programs to create and destroy files at a determined rate and for other programs to watch this with a degree a constancy in order to extract the rate of change. Although the bandwidth of a covert channel may seem small, its use over time may allow it to be an effective means to subvert the established information distribution channels.



The general techniques used to prevent covert channels can directly apply to the IW functions. This would include having the IW create the identifying codes for PIUs. The key words in the identifying information section of an IPT should be updated by human action when the PIU is not opened, otherwise the information in a PIU could quickly escape by an automated process of coded key words.

#### 4.4 Internal Controls for Watchdog Resident Devices -- Other Processing Architectures

##### 4.4.1 Multiple Information Watchdogs in a Single Device

A separate IW is required for each reconfigurable device. It may be advantageous for non-reconfigurable subassemblies of a device to also have their own IW. For instance, in a multiprocessor device, the distribution of processing may be enhanced if each processor has its own operating system (which includes the IW). In such a trusted environment, each processor-IW can be thought of as being a part of the overall device-IW. All of the resources of the device can be made available to an application program running on one of the processors by that processor's IW coordinating activities behind the scenes with the other IWs. IWs keep track of their own status through tables -- LC IACL Table, Information Memory Assignment Table (IMAT), PIMA Access Allowed Table (PAAT), etc. The coordination of IWs can be facilitated by having these tables belonging to each subassembly-IW easily accessible to all other subassembly-IWs in a device. This may best be accomplished by having a separate standard component hold the commonly accessible tables. This component can also include the arbitration control function. The type of resource sharing is not developed here, the main point being that many IWs can exist within a single device and that they do not need to communicate with each other using the channel developed in Chapter 3.

#### 4.4.2 Information Watchdogs in Multiple Devices

The transfer of protected information between reconfigurable devices involves the transfer of an encrypted PIU. All of the device management functions may be needed to properly send and receive the PIU regardless of the type of receiving device. There are two general types of devices -- independent devices and dependent devices. Independent devices decide on their own how to handle received information based on the contents of the IACL section and the identifying information section of the IPT, and based on the protected information. Dependent devices are told by the sending device how to handle the received information. These instructions are contained in the "receiving device specific instructions" (RDSI) section of the IPT as was first discussed in Section 2.6. The instructions in the RDSI can vary greatly -- from a request to execute a certain application program, to the memory locations at which to store the information. In all cases the receiving device must perform the information, memory, and processor management functions needed to follow the directives in the IACLs of the received PIUs.

The channel separating reconfigurable devices imposes new requirements not present with processing occurring within the same device. The need for device management functions was mentioned. Memory management is also affected. Within a device, the opening of PIUs and PIMAs causes a context switch. While that context is active, memory can be accessed by simply specifying an (allowed) address. The receipt of a PIU on a channel can be analogous to the opening of a PIU at a device. Each receipt of a PIU causes a new context switch (if the context does not actually need to be changed then this operation is more innocuous). The computation of the LC IACL by information management, therefore needs to be performed on the receipt of each PIU.

#### **4.4.2.1 Prevention of Covert Channel in RDSI Section**

The RDSI is specified by the sending device's application program based on the contents of protected information. The RDSI can therefore be used to code the contents of the protected information. The RDSI is part of the IPT, and since the IPT is encrypted, the RDSI can not create a covert channel during transmission. At the receiving device though, the RDSI can alter the configuration of the device. If other programs at the receiving device can detect the change in configuration, then a covert channel exists. There are two complementary ways of preventing this. One approach requires that when an application program is validated for its usage influence, the independent auditor also must ascertain that the program does not purposefully code the RDSI section to reveal the contents of the protected information section. The other approach only allows RDSI commands that do not cause a device configuration change that would be perceptible to another program on the device, or a program on another device trying to use the device.

#### **4.4.2.2 Serial Bit Stream Between Devices**

The channel between IWs of reconfigurable devices should be thought of as serial. The protected information, the IPT and the RDSI should be serialized and encrypted prior to being transferred to another IW. A serial physical channel is used over relatively large distances to avoid the difficulties involved with synchronizing the reception of signals sent over parallel lines. The rate of transfer over a serial channel may not be as fast as that over a parallel channel. Therefore a physical interface for a parallel channel directly between IWs in close proximity should be standardized. The serial stream can be sectioned into various bit widths where a particular line has no specific purpose such as being an address line. Physical optical serial channels between IWs can retain the intrinsic serial nature of the communications.

### 4.4.3 Simple Devices

An IW at a device only needs to perform those functions which are required to follow the instructions in an IPT. A device can be designed to perform processing in a limited way so that some IW functions do not need to be performed. The simplest device only requires device management to send or receive a PIU. The other management functions are not needed since:

- In terms of information management, only PIUs with a specified IACL are accepted.
- In terms of processor management, there is only a single application, or multiple applications all with the same usage state.
- In terms of memory management, there is only a single PIMA with a set IACL.

The IW must check that the incoming PIU has the required IACL, let the device do whatever it wants to do to the information, and then logically attach the IACL to any information leaving the device.

## 4.5 Examples of System Use

### 4.5.1 Control of Flow and Access of Information

This example illustrates some of the information watchdog functions involved with controlling the flow and access of information. In order to put faces on the parties in the following scenario, party A may be the order entry department at a mail order retailer, and the information in its possession may have been generated during a credit card sales transaction. Party B may be the record keeping department of the issuer of a credit card which was used during the sales transaction. Party C may be a marketing department within the credit card issuer. In order for information to securely flow between these parties, certain procedures are performed by an IW.

The PIU at device A. In the past, party A has entered into an agreement with party B that if party A is involved in originating information or comes into possession

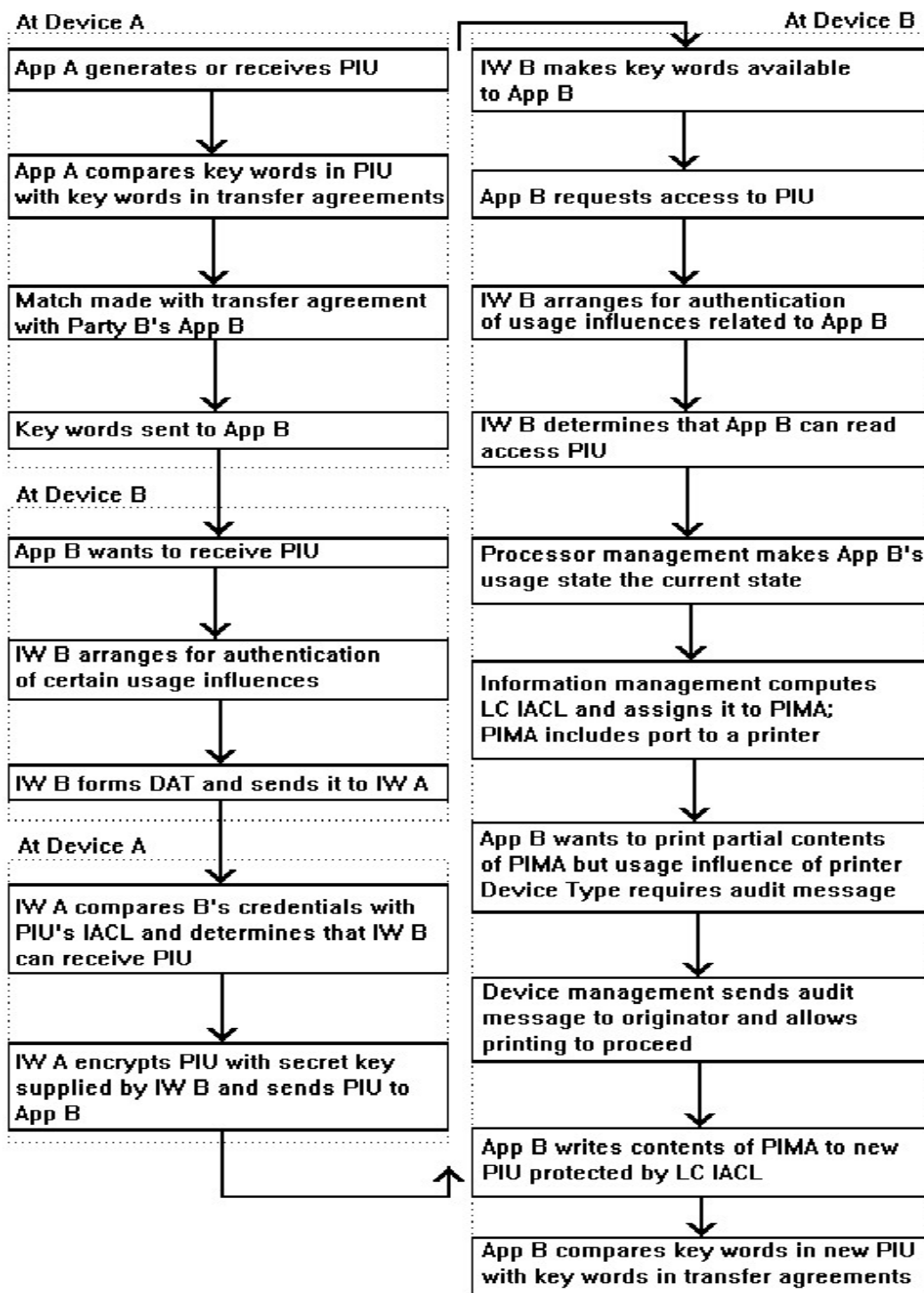


Figure 4.7 Example of steps to control flow and access

of information of a certain type, party B should be informed. Application A is handling the information on party A's device A and application B is handling the information on party B's device B. Application A has a PIU of possible interest to application B. Application A has determined this based upon a matching of the nonconfidential items in the IPT with key words supplied by party B. Application A sends a message consisting of selected items from the PIU's nonconfidential items to application B and asks for device B's device authentication token (DAT). Application B decides, based on the nonconfidential items, that it wants to receive the information and so it has its IW arrange for the authentication of certain of its usage influences. The IW places the validated device tokens into a DAT and sends it to the IW on device A. The IW on device A compares device B's credentials to the PIU's IACL and determines that device B can receive the information. The PIU is encrypted and sent to device B.

The PIU at device B. The IW at device B deciphers the PIU. The IPT and protected information are stored for further reference. The stored data must be encrypted with the IW's public key or with a symmetrical key (this encryption operation should be invisible to other processing). Since the PIU was sent to application B (using application B's PSAP address), the nonconfidential key words are made available to application B. Application B decides that it wants to access the PIU. The IW at device B arranges for any needed authentication of usage influences related to application B. The IW then determines that application B can read access the PIU. If application B's usage state did not satisfy the IACL, application B would be informed of the arrival of the PIU and be allowed to access the nonconfidential items but would not be allowed to access the PIU. Application B at periodic intervals processes the recently arrived PIUs. The IW first applies processor management to make application B's usage state the current state of the processor. Application B opens the PIUs along with a PIMA for work space. The IW's information management function computes the LC IACL and

assigns it to the PIMA. The IW then applies memory management during processing to maintain the integrity and confidentiality of the protected information in the PIMA. Application B during the processing wants to print some of the information in the PIMA. The defined PIMA would need to include an address which acts as a port to a printer. Information management before assigning the LC IACL to the PIMA would need to have checked that the LC IACL includes a usage state with the printer Device Type usage influence. At this point it is noticed that the printer Device Type has a control attribute which requires that an audit message first be sent to one of the originators. The IW sends the audit message and then allows the information to be printed. Application B then opens a new PIU with the LC IACL and writes the information in the PIMA to the PIU. Application B then wants to send the new PIU to application C on device C and so formulates a message using the nonconfidential items to inform application C of the existence of the information. Some of these steps are shown in Figure 4.7.

#### 4.5.2 Compensation for Use of Software Product by End User

Taxation Software Company (TSC) sells a tax return preparation program. There are two methods for a consumer to purchase the use of this program -- per use or unlimited use.

The per use method illustrates the use of the originators link section to control access to information. To implement a per use method, TSC has included its device ID in the originators link section of the IPT. It has also specified in the IACL section a single usage state consisting of the single usage influence of the Device Type the program can run on. Within the read access control attribute which accompanies the Device Type (see Section 2.4.4.2), TSC specifies that prior to the loading of the program an audit message which accomplishes payment is to be sent from the user to TSC (see Section 2.5.2.3). The program is then made accessible to the processing unit. At a

certain determined completion point, the software completes its execution until it is made accessible again via a payment message. There is no restriction as to the number of computers or people that can run the program -- for each prepared tax return, TSC is compensated.

The unlimited use method illustrates the great flexibility in which allowed users can be specified via an IACL. It also illustrates the ability of control attributes which are associated with usage influences to control processing at a device. To implement an unlimited use method, TSC can offer various plans for the installation of its program. A user effectively selects a plan by including selected device tokens with its order message. When the program is transferred to the user, the selected installation plan is specified via the program's IACL. Possible installation options are:

- Unlimited company-wide use -- The IACL contains the Administration usage influence.
- Limited company-wide use -- The IACL contains the Administration usage influence along with a control attribute specifying the total number of copies allowed.
- Device specific use -- The IACL contains the Device ID usage influence for one or more specific devices.
- Person specific use -- The IACL contains the Person ID usage influence for one or more specific individuals. Each specified individual can install the software on each device to which it has transferred its Person ID.
- Person specific use with presence at device -- As above but each device must have approved biometric identification technology and the user must identify himself as being present at the device before access to the program is allowed (see Section 3.4.7.4).



### 4.5.3 Transfer of Music to a Compromised Device

This example illustrates protection mechanisms which can lessen the damage done by a compromised device. A user presents a purchase request to a music distributor for a musical selection. The distributor presents various distribution options to the user. Based on the choice of an option, the user presents device tokens to the distributor which are used to limit the distribution of the musical selection. For instance, the submission of device ID tokens would limit the distribution of the music to specific devices. Likewise the playing of the music can be allowed at any device as long as particular people are biometrically identified as being present. The musical selection along with its IACL is sent to the device signing authority for the type of device which will play the music (see Section 4.2.3.4). The musical selection plus IACL after being signed is returned to the distributor where the PIU would be encrypted with the public key of the intended user's IWD. The resulting data can either be transferred to the user over a transmission channel or on a storage disk.

Unfortunately for the generators of the music, the user who receives the encrypted PIU has managed to successfully extract the private key of the recipient IWD. The user by applying the private key to the PIU is now in full fraudulent possession of the digital musical code. In order for the code to be of use, it needs to be accepted by a device which can create an acceptable audio output from it. The musical code is fraudulently transferred to a legitimate device which first checks the integrity of the IACL by verifying the device signature. At this point, the device will refuse to accept the information either because the IACL has been switched in which case the signature will not be verified or the proper IACL is present but the required usage influences as specified in the IACL are not present at the device.

Some counterfeit devices may be available which will accept the extracted digital code. The number of counterfeit devices can possibly be kept down with controls over

component distribution as well as with the efforts of the law enforcement community. If periodic security inspections or updates are instituted then the compromised device which originally extracted the music code will in time be put out of commission (see Section 4.2.3.1).

#### 4.6 Adding Functionality to the Information Watchdog

The function of the information watchdog is to carry out the explicit or implicit instructions in the information protection tag. In order to keep the overhead related to the size of the tag as small as possible, the instructions in the tag should be complex in the sense that in order to carry out an instruction, a string of more basic instructions (or logic functions) must be executed. In terms of high level programming languages, this conversion is done with a compiler. Although the basic instructions may remain the same, any change in the high level language, requires a change in the compiler. Both the interpretation and execution of information protection tag instructions are done in the information watchdog.

The information watchdog can be designed using various approaches -- from fixed logic gates to a microprocessor running software. A fixed logic approach would require new equipment for each new version of the information watchdog, since a modular and hence replaceable sub-assembly would provide an easy avenue for watchdog tampering. An approach involving a microprocessor running software allows for easy upgrades. Where a microprocessor exists in a device, the information watchdog could be implemented as an operating system or as a suite of modules which would interface with an operating system.

An approach for creating a controlled update process for software can make use of a certification authority as discussed in CCITT X.509 [7], and applied in Chapter 3 to the device authentication procedure. The information watchdog can have securely

placed in it, the public key(s) of the certification authority. Valid software or firmware updates would be digitally signed by the certifying authority or by its delegate. The update could be sent through a telecommunications network.

## CHAPTER 5

### CONCLUSION -- PATHWAYS TOWARD GENERAL ACCEPTANCE AND TASK PLANNING FOR SYSTEM DEVELOPMENT

#### 5.1 Pathways Toward General Acceptance

The Protected Information Environment (PIE), is technology dependent. In order for it to reach its potential, information watchdog resident devices must saturate society. Similar to the telephone system, each new "subscriber" adds value to the system by increasing the level of connectivity available through the system. The ultimate in this regards is universal service. Generally, with the telephone system, a connection is made between two parties. With the PIE, in order for information generated in a transaction to be processed by all concerned, a connection must be accomplished between multiple parties -- this may more aptly be stated as all parties concerned must possess compliant equipment. Therefore in contrast to the telephone system, the PIE requires more of an all or nothing societal implementation for it to be useful. On the other hand, the telephone system, in addition to requiring customer premises equipment also required that a transmission and switching infrastructure be developed and implemented. The PIE can piggyback on the existing and future telecommunications infrastructure as well as on other communications channels.

A pathway of gradual implementation for the PIE is highly desirable. Those uses of greatest need can create markets to support the initial development of the various concepts which comprise the PIE. An initial development phase is needed to verify the effectiveness of the concepts before they attain general acceptance.

It was mentioned that in order for the subsequent processing resulting from a transaction to be executed with the PIE, all processing equipment must be information watchdog resident devices. Therefore, in order to create a PIE before the PIE is created, a class of transactions must be identified which result in a moderate degree of subsequent processing. A very limited degree of subsequent processing can be controlled with traditional secure computing and administrative procedures. A high degree of subsequent processing creates the need for a seemingly boundless number of compliant devices.

An area where a moderate degree of processing results is with a large product development project within a single firm or among a few cooperating firms. The aim here is to protect the trade secret variety of private information. The value placed on the security of this type of information is great enough that a firm might be willing to accept the greater cost of information watchdog resident devices -- during the initial development phase, in addition to an inherent overhead cost, there will also be a developmental cost.

Virtually all aspects of the PIE can get a workout under these conditions. Usage states may consist of a number of usage influences. It is important to try out a number of usage influences, not only to test the general concept but to test the validation approaches -- each usage influence is validated based on its unique characteristics.

A helpful development that can make use of the control attribute feature would be to only selectively allow information to be printed (or output in other ways). This is because once information leaves the system in an authorized way such as a report printed on paper, the system can no longer control it or keep an audit trail on it. Instead, as the general case, reports can be "printed" to an electronic report presenter such as are being developed for pen based computing. The ideal here is to supply the convenience of printed output while preventing the information from leaving the system. For the

business firm that doesn't want its secrets leaving each night in a briefcase, a location usage influence can restrict the functioning of the report presenter to the premises of the business (possibly implemented via some form of radio signaling).

The tamper proof aspect of the information watchdog may be of interest to certain companies that rely upon the capture of information in possibly hostile environments. The resource usage meter may be updated to provide for the transmission of meter readings to the offices of the utility company. This requires that the meter securely guard its identity and send messages which have their integrity secured. Secure communications can be achieved through public key cryptography. The meter's identity can be guarded and private key kept secret through embedded information techniques. Usage influence concerns are often not present with meter information -- the consumer is under the impression that the information isn't used much beyond that of preparing a bill. With the ability to read a meter in real time from a location remote from the meter, the information takes on new concerns. Likewise if meters start measuring information usage rather than just utility usage, the meter reading portrays private information. Therefore the meter of the future may need to include some way to generate information protection tags and to be able to authenticate the receiving device.

After the concept and technology is proven, there needs to be a catalyst for it to gain acceptance by the general public as a necessary feature of information processing equipment. As stated earlier, the effectiveness of a single compliant device is dependent upon the existence of a compliant device in the hands of all those diverse parties that will have a need to process the generated information. It is almost that the saturation of society with compliant devices must be a single event consisting of the simultaneous purchase of such equipment by each organization and each individual.

Such a single event could result from the mandate of federal law. In the absence of this, the route towards saturation will probably consist of a gradual process leading

to a threshold level. The process can be facilitated by coordination. It can not be expected that coordination will come from the general public or from the major users of private information. However, there is a great deal of motivation for the creators of proprietary information to coordinate their efforts so that information processing equipment contains an information watchdog. If the hardware developers were the same as the software developers the need to protect intellectual information would find a more direct path towards satisfaction. Nevertheless, the value of hardware is largely derived from its ability to execute or more generally accommodate software. A coordinated effort among software developers can result in the hardware developers agreeing to manufacture compliant devices. The need for software developers to supply the installed hardware base with product upgrades diminishes the unified front. Software developers may be willing to accept the possible misappropriation of their product in order to make a sale. This is particularly true if the willingness to decline a sale is not shared with a competitor. Therefore the introduction of compliant devices as a way to protect proprietary information will be gradual. During this time the growing installed base of compliant devices will have a minimal impact on how private information is processed. Once a threshold is reached though, the use of such equipment will be considered a standard requirement for the processing of private information. This pressure may finally result in the saturation of society with compliant devices.

## 5.2 Task Planning for System Development

There are a number of tasks which must be accomplished in order for the Protected Information Environment to be realized. The project of developing the technology for the PIE will be broken down into tasks and the necessary skills to accomplish each task will be discussed. Each task requires an amount of time, i.e., person-months, in order for it to be accomplished. This amount of time can not be predicted perfectly due to unforeseen problems and serendipities, usually problems.

Therefore in addition to an average time estimate, each task will be assigned a risk factor. A four category scale which is used to assign risk is given in order of increasing risk:

- Off-the-shelf. The technology already exists in product form. For the most part it is assumed that the make/buy decision should come down on the buy side. For this category, risk is minimal, and the time needed to acquire the technology is considered minimal as well.
- Development. The procedures to accomplish a task in this category are well established. A fairly accurate estimate of time can be made by referring to the performance of similar tasks carried out in the past. Due to the complications imposed by time itself, the greater the estimated time period, the greater should be its variability.
- Shared research. New ground is being investigated so the time to accomplish this category of task can be estimated with less of a degree of accuracy. Tasks in this category are being investigated by other projects. Where reliance is essentially placed on the success of others, this category can also be described as external research. The efforts expended by others can influence the amount of time and risk involved in having the task successfully completed. By giving up some control, the risk factor can increase, but generally the resources supplied by others are considered to decrease the required time as well as the risk.
- Specialized research. New ground is also being investigated here but in this case the problem to be solved is specific to the project. This category poses the most risk. The solitary effort can lead to narrow vision and wherewithal.

Any assignment of person-months would need to be preliminary as the backgrounds of the people assigned to each task can greatly influence the time needed for the completion of a task. Where the individuals bring a background of relevant



experience, their inputs may improve the accuracy of a time estimate. To give a feel of the perceived magnitude of the effort, a time estimate will be given for each task in estimated person-months. All off-the-shelf tasks will be assumed to take an insignificant amount of time. Another important aspect is that all of these tasks can be worked on concurrently; within a task, sub-tasks may need to be worked on consecutively. The result will be a prototype with the finished product and production line to follow. The following tasks need to be accomplished:

#### 5.2.1 The Information Distribution Directory

The IDD contains the groupings of information usage influences. This is essentially an online hierarchical data base. Such technology readily exists today and so poses an off-the-shelf risk.

#### 5.2.2 Biometric Technology

Biometric technology is needed either as an imbedded function of an IW protected device or as a specialized device which can easily communicate via I/O ports with an IW protected device. This task is considered a shared research risk category approaching an off-the-shelf risk category. If the biometric function is carried out in a specialized device then the device will need to be designed so that it can securely communicate with the IW protected device. The tasks required to accomplish that are found among the tasks to design an IW protected device.

#### 5.2.3 Encryption Techniques

Asymmetric and symmetric encryption techniques are needed. This is considered an off-the-shelf risk category. A company has been established to license the technology of the RSA asymmetric encryption scheme and some software products are

incorporating its functionality. The estimated person-months is 6. If the advantages of having an IW generate its own public/private key pair is established, this would be a task for shared research.

#### 5.2.4 Outer Casing of an IW Protected Device

The development of the outer casing of an IW protected device requires the expertise of a materials engineer (see Section 4.2.1). A material must be selected which can be shaped to surround an electronic assembly of various shapes and dimensions. For a given casing, resistivity must be able to be consistently measured. This task belongs to the specialized research risk category. The estimated person-months is 10. Instead of the entire electronic assembly being securely encased, only a single arithmetic-logic and encryption unit may need to be, thus resulting in a form factor of a multichip module.

#### 5.2.5 Inner Casing of an IW Protected Device

The development of the inner casing of an IW protected device requires the expertise of an electromagnetic compatibility engineer. Electromagnetic radiation should be prevented from leaving the device so that the plaintext contained within it is not revealed, and electromagnetic radiation should be prevented from entering the device so that its operation is not altered. Such issues have been a concern a while in regards to military electronics (with the U.S. government's TEMPEST specifications) and in regards to civilian electronics (with the FCC's specifications). It is considered that the task falls somewhere between the shared research and off-the-shelf risk categories. The estimated person-months is 10.

### 5.2.6 Controlled Manufacturing

A manufacturing facility will need to be set up that can control the production of IW protected devices. The main objectives are that the device is produced according to specifications, that the IW is programmed with the correct public key of the certifying authority, and that the device is programmed with a securely composed private key or code without it being revealed outside of the device. Automated manufacturing facility design expertise is needed to accomplish this task. This task has aspects of development risk and specialized research risk. The estimated person-months is 12.

### 5.2.7 Compliance with Environmental and Quality Standards

Currently the Western European countries are taking the initiative in devising compulsory electronic product standards in the areas of the environment and quality. Compliance with international standards is necessary in order to market the system worldwide (if the U.S. export ban on products with public key cryptography is ever relaxed). In addition, abiding by such standards can result in a superior product. Knowledge of the standards should be applied at all stages. No foreseen problems exist with regards to following the standards, other than the inability to functionally recycle components in IW compliant devices. This task poses a development category risk. The estimated person-months is 5 spread out over the life of the prototype development.

### 5.2.8 Operating System of an IW Protected Device

The internal functioning of the IW has been described in this paper and to implement it requires a developmental effort by programmers. The interface with a particular operating system has been less well defined and carries the risk of somewhere between the specialized research and development categories. The estimated person-months is 50. The development of the operating system is the most involved task. To further describe the sub-tasks that are involved, Figure 5.1, at the end of this

chapter, displays a time line. Each sub-task requires a single programmer or systems analyst, except the sub-task to integrate all code requires the simultaneous efforts of all those who worked on the preceding sub-tasks (a staff of four). The detailed design sub-tasks are guided by the functionality described in Section 4.3. The operating system selection sub-task should select an OS to which the source code can be accessed and modified. This sub-task should also be attentive to the class of the OS under the Department of Defense Trusted Computer System Evaluation Criteria [19].

### 5.2.9 Electronic Hardware Design

The electronic hardware requirements can make use of off-the-shelf parts and a development effort by digital design engineers. The component to measure the resistivity of the outer casing may involve specialized research risk. An IW protected device can have a wide variety of functionality. The effort to develop the functionality itself has a great impact on development time. For the purposes of the first IW protected device, a previously developed, well understood, general purpose device should be selected. The IBM compatible PC meets the criteria. The estimated person-months is 12. If only the information watchdog is made a secure component as is described in Section 4.2.3.2, then the development of an ASIC possibly containing both the ALU and the encryption unit will require substantially more time.

### 5.2.10 Information Usage Influence Verification: Location

The presence of a usage influence at a device must be verified in order for a certificated token to be formed. The method of verification for each usage influence can be different and it usually will involve some form of technology. As the universe of UIs can evolve over time, new methods of verification will be devised over time.

An important usage influence could be Location. As described in Section 3.4.7.5, the round trip time of transmission, from a base station of a cell to a device, could

effectively verify location if the round trip time is less than a certain value. To develop such a method would require the same skill set as is required for cellular communications. This task falls in the shared research risk category and it is envisioned that the cellular or personal communications industry would want to offer such a service as a simple extension of their business. The need to supply all areas with a cell of less than a certain size poses the greatest difficulty. Within an office building, the same technology can be offered, with a much more limited infrastructure problem -- one building can be one cell. The estimated person-months is 12.

#### 5.2.11 The Model of Information Flow

The paper offers a model of information flow which as a first pass is considered a completed task. Its usefulness and efficacy can only be tested with actual use. The flow of information can be thought of as tracing out a network with many nodes. If the behavior of each node could be represented by some form of mathematical model, then the network could be simulated to see how various network topologies result in optimizing some desirable state of each node.

Each node, though, can be unique in many ways, particularly when a node is a human being. Understanding the behavior of a node may defy, at least for awhile, attempts at mathematical modeling. This is largely because people are often not aware as to what is desirable until they have fully experienced several options, and even then tastes may change. The implementation of an actual system does provide more of a closed environment for study; more importantly, since parameters of the system can be controlled, an actual system would provide a laboratory for experimentation. Such empirical results could possibly allow for a degree of mathematical modeling and simulation.

The elapsed time to complete this development effort is controlled by the critical path which is completely comprised of the operating system development task. As

shown in Figure 5.1, the total elapsed time is 72 weeks or one and a half years. In addition to all of the preceding tasks which directly influence the development of the prototype there are many indirect tasks which will need to be performed for an organization to function.

Graphic no longer available.

Figure 5.1. Time line of critical path for system development

## **APPENDIX**



## **APPENDIX A**

### **HIGHLY TRUSTED INFORMATION SYSTEMS**

#### A.1 Introduction

The Protected Information Environment (PIE), as described in the preceding chapters, was developed by extending computer security concepts to the universal distributed non-trusted environment. The PIE is meant to be a flexible system which can be relied on in many situations to protect both private and proprietary information. An alternative but more limited approach to providing information protection in the everyday world is to put reliance on Highly Trusted Information Systems (HTIS). An HTIS is geared towards protecting private information and only protects proprietary information in a minor way. An HTIS operates in a limited environment, and so it does not require the security extensions which create the PIE. As a secure system, the HTIS still needs to implement various security concepts such as access control lists, audit trails, and cryptography.

The PIE is a mass produced solution which is available to all with the willingness to pay a (hopefully small) overhead fee on processing equipment and communications services. The HTIS is only available via information processing organizations that are willing to assume a fiduciary role in how they handle their client's information. Normally, a fiduciary responsibility is associated with an individual or close group of professionals who center the service offered around the needs of the client. In this case the client's need is for information privacy. This chapter proposes a way of controlling information availability within organizations of varying complexity so that a high degree of responsibility can be reached. As always, this fiduciary role needs to be balanced

with the HTIS's goal of running a successful business, and this fiduciary role will need to be balanced when an HTIS acts as a dual agent, representing more than one party in a transaction. The processing that an HTIS will perform on a client's information must be specified in advance and agreed to by the client. The fiduciary responsibility is primarily carried out by an HTIS by maintaining a secure system and by abiding by its agreement with the client. Independent audit surveillance can ascertain that these responsibilities are being met.

#### A.1.1 Organizations that Can Implement an HTIS

The HTIS can apply to a broad spectrum of organizations but it has particular value to those organizations built around performing a highly defined information processing activity. This is advantageous to the client since the highly defined nature of the processing gives assurance as to the limits of the processing. This is also advantageous to the offering organization since it can tinker with its processing architecture (subject to demanding design guidelines and independent audit surveillance) without being subjected to the unyielding demands of a fixed information protection tag. As an example, the information processing activities needed to operate a telecommunications network are highly defined.

All organizations can implement an HTIS, from the local mom and pop store to the multinational corporation. An individual or organization acting in the client role may find it undesirable to have to rely on all these HTISs. As explained later, an HTIS can interface with the PIE or with other HTISs in such a way that it can act as an intermediary between the client and involved (third) parties. The client can put primary reliance on the intermediary. It is advantageous for all organizations to design their information processing activities as an HTIS so that they can access more sensitive information items.

### A.1.2 Key Unit of Information -- The Activity Information Unit

Instead of the PIE's PIU, the HTIS has an activity information unit (AIU). For a highly defined information processing activity, analogous to electrons, AIUs flow through an information processing circuit to accomplish a certain function. All HTISs must have highly defined processing whether or not it is innate to the organization and so the concept of the AIU will apply to all HTISs. The development of the concept of the AIU is the primary objective of the appendix.

AIUs directly reveal something about a client. In addition to AIUs, an HTIS may also process system information (SI). SI does not reveal anything about a client other than that which can be surmised by the client being a subscriber to the service which uses the SI. A client's access of a data base is an AIU but the data base (if not containing information specific to the client) is SI. Since the client's status as a subscriber can be hidden from the outside world, SI should not compromise a client's privacy.

### A.1.3 Objective of the Activity Information Unit

It is possible for an HTIS to accomplish its responsibility of securely restricting the availability of the clients' information by using traditional security concepts with the additional use of independent audit surveillance. The primary security issue is how to control information availability to organizational personnel and concern over information exposure to non-organizational interlopers is a secondary issue. This is because during the authorized access of information, plaintext is exposed, at all other times information can exist in an encrypted form. Traditional security concepts can control information availability with user identification in conjunction with access control lists, and by restricting the implementation of physical channels which make possible the flow of information to I/O devices and by physically restricting human access to I/O devices. Control over information availability can be enhanced though by

considering another issue. The issue that remains is how should information be apportioned so that access restrictions can best be specified -- what are the general principles that determine how information should be assigned to different AIUs? The makeup of an AIU is not a self contained decision but is dependent on the information processing architecture. In order for an AIU to effectively allow for limited availability of information, an information processing architecture should be designed around the concepts of topology, aggregation, and stationarity. Each of these will be discussed in the following sections.

### A.2 Principle of Topology

Just as a computer system can be secured through the use of protection rings as described in Section 4.1.1, an HTIS can consist of rings of access. The inner most ring has access to all the information related to the provision of a particular service to a particular client. Each succeeding ring has access to fewer and fewer information items. The inner most ring should consist of the client's information system, and the outer most ring should consist of the information systems of involved parties. The middle rings should consist of various degrees of information accessibility within an HTIS. This ring structure is illustrated in Figure A.1. The restriction of information access for these three basic ring classifications is accomplished through physical separation. For the middle rings within an HTIS, the restriction of information access can be accomplished with both physical separation and with access control lists. Generally, as is possible, as much information should be processed at the client, and as little information should be processed at involved parties. When the system is designed, the functioning of all rings, including those of the client and the involved parties, must be considered in an integral manner. It may not be necessary for information traveling from one ring to another ring to be handled by processing functions situated within intervening rings. Doing so may

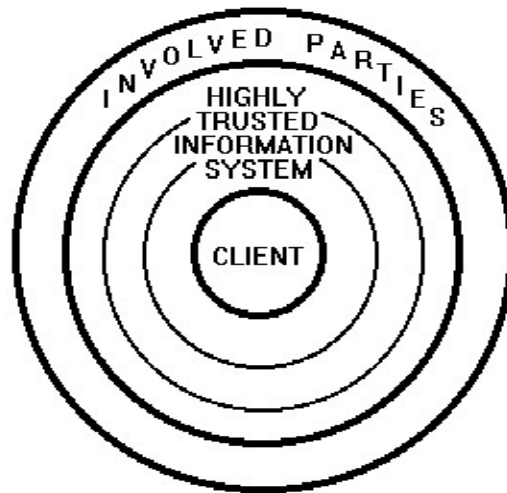


Figure 1.1 Hierarchical Information Processing Topology

help maintain the structure of the system, but it may also allow for unnecessary information exposure and less efficient processes.

Each AIU which enters an outer ring is related to the parent AIU by a code. This code is called a Transaction Anonymous Code (TAC). The more complete inner AIU is in a sense the author of the outer AIU, and the code allows for the inner AIU to be anonymous to the outer ring. Over time, an outer ring may have need to relate AIUs sectioned due to the principle of aggregation (to be discussed later). In order to accomplish this an Activity Anonymous Code (AAC) can be assigned to AIUs.

#### A.2.1 Information Flow from an HTIS to Involved Parties

Involved parties, external to an HTIS, exist in the outer most ring. The flow of information to involved parties must be agreed to by the client. An HTIS in such cases can be considered an intermediary between the client and the involved parties.

The intermediary's job is to release only those information items necessary to complete a transaction for the client and to hide the client's identity by using anonymous codes to form a link between the hidden party and involved parties. The key advantage

of the intermediary is the latter, the ability to shield a client, since the former, holding back information can be done with PIUs (where the PIE has been implemented). For instance, when engaging in an information generating transaction, two or more PIUs can be created. The PIUs can contain mutually exclusive information or can be built upon one another with progressively more sensitive information items included. The IACL would become more restrictive as the information in the PIU becomes more sensitive.

The TAC and AAC have special importance when dealing with involved parties as a way to hide the identity of a client. In some cases an involved party has no right to tie-in the client with a transaction. The TAC can be used here. For instance, a broker acting as an intermediary can hide a client's identity. With location related services, such as cellular telephone and automatic vehicle identification, an HTIS can protect the privacy of a person's location by representing a transaction with a TAC.

In other cases, the hidden party's activities may need to be related and so is assigned an AAC. For instance, a hospital does not require that its computerized records have an absolutely identifying code of a person such as a person's social security number but it must be able to gather in conjunction with other hospitals and doctors the medical records of a patient in order to form a medical history. Besides health care providers, other parties such as health insurance companies may be entitled to this information. Another use of the AAC can involve purchase transactions. For instance, a person may wish to engage in an anonymous relationship with an airline. The anonymity helps prevent burglars with access to the airline's data base from knowing when you and your family are away on vacation. The relationship allows your mileage flown on individual flights to accumulate in your frequent flyer account. It should be emphasized that on a personal level, when anonymous codes are in use, people can still address each other using personal names according to custom. The main concern is with computerized information which can be so easily reproduced and distributed.

In order to implement such a scheme around TACs and AACs, certain logistics must be worked out. For instance, transferring funds to an intermediary may compromise privacy, so fund disbursements may need to be made through a financial (privacy) intermediary, external to or a separate entity within a more traditional type of bank. The transfer of physical items, such as letters, between end parties can make use of the post office box. The post office box, or a similar privately run service, is a traditional approach for providing anonymity to recipients of mail, but with the service provider's new formal role as a privacy intermediary, its record keeping must be tightly controlled.

The big picture which the AAC helps to create by relating different pieces of information increases the possibility of a breach of security but an interloper operating external to the system or within an outer ring would need to accomplish two tasks -- gain access to information and associate it with a person or organization. Such discoveries still have traces of conjecture and can only affect a portion of our society's vast number of transactions. Information referenced with a TAC can be very secure, though.

#### A.2.2 Encryption Across Hierarchical Rings

Information which is transferred from an inner ring to an outer ring can be protected in ways other than the filtering of items of information. Within the transferred AIU some of the information items can be encrypted. If the outer rings job is to transmit a message within a network, then at the end of the journey, the AIU can be transferred back to the inner ring where the encrypted information can be deciphered.

In CCITT Recommendation X.402 [18], Message Transfer Agents can encrypt a message to form confidential electronic mail, both in terms of message content and the identities of sender and receiver. CCITT Recommendation X.402 describes the Message Flow Confidentiality security service, "This security service provides for the protection

of information which might be derived from observation of message flow.... The Double Enveloping Technique enables a complete message to become the content of another message. This could be used to hide addressing information from certain parts of the MTS".

### A.2.3 Placement of System Information

Many services involve the query of a data base which contains information of a non-revealing nature in regards to the client. The convergence of a client's inquiries at a data base may be revealing though. This can be illustrated with the system information of a data base of current stock prices and the service of computing a portfolio's value for analysis. There are a number of variations but two will be considered:

- The data base and processing for portfolio valuation could be contained within a ring of the HTIS. This would make the contents of a client's portfolio available to all authorized people at the HTIS.
- The entire data base could be transferred upon demand to the client's computer were the processing function would be carried out. The client's accesses and processing would not be revealed beyond the inner most ring.

The movement of data for the purposes of maintaining privacy, needs to also take into account efficiency. Some SI with great client demand can make use of broadcast media. In general though, the implementation of high bandwidth channels should make efficiency less of a concern.

### A.3 Principle of Aggregation

Aggregation is concerned with the degree to which information relating to an individual client is gathered together for inclusion in an AIU. A particular service involving a client should be factored into various activities. Each activity should be mutually exclusive to other activities as far as processing is concerned, although they may form a single service as viewed by the client. Many transactions involving a



specific client can relate to the same type of activity. Instances of transactions of the same type should as well not be aggregated, where possible, into a single AIU. The Activity Autonomous Code (AAC) is actually contrary to aggregation minimization since it relates transactions, but depending on the situation there may be other valid reasons for justifying it. Therefore, both type of transaction (billing record and medical diagnosis record at a hospital) and instance of transaction (billing records for different visits to a hospital) are determining factors in the creation of an AIU.

The problem to be minimized is that the more information that is included in an AIU, the more complete is the picture painted of a client; the synergistic nature of information aggravates the problem. Aggregation isn't just concerned with how information is stored but also with the availability of systems which can lead to the aggregation of information. Whether a system user's request for information results in an access to a single storage device or to the automatic gathering of information from various storage devices on a network, the degree of information exposure is the same. The division of a topologic ring into separate AIUs is shown in Figure A.2.

The purchase of a product can illustrate the principle of aggregation. The overall sales relationship that the retailer has with the customer is called a service. The service consists of various types of activities, such as billing, warranty, maintenance reminders, etc. Each time that a sale to the same customer is made, an instance of each type of activity occurs. Disregarding for now the principles of topology and stationarity, each instance of a type of activity is an AIU. Where AIUs need to be integrated, AACs can be assigned. Since the integration of AIUs is counter to the principle of aggregation, the principle of topology can assist by allowing access to an integrated AIU to occur at an inner, more trusted ring. The ideal is for the aggregation to occur at the inner-most ring -- the customer's computer. For instance, billing can be settled on a per transaction basis

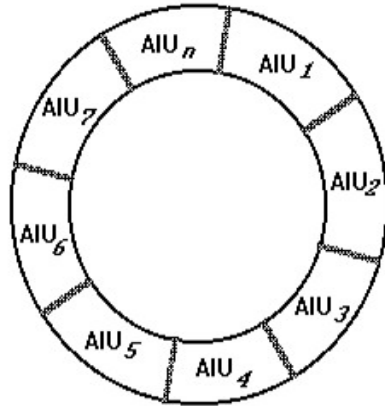


Figure A.2 An information service should be factored into separate processing activities.

using some form of automated funds transfer and the HTIS can provide the client with specialized software or suggest a standard product for the processing of accumulated past transactions at the client's computer. The reference link between a billing AIU at the customer and in the HTIS can be made using a TAC.

#### A.4 Principle of Stationarity

If AIUs are stored for a relatively long time, especially in an on-line data base, then the possibility of compromise is greater. Ideally AIUs should be kept on-line only for as long as is needed. This generally includes the time needed to complete the transaction to everyone's satisfaction. AIUs may need to be retained to form an audit trail needed to help safeguard the integrity of data in a data base. There are other reasons to retain AIUs, such as possible legal and taxation requirements.

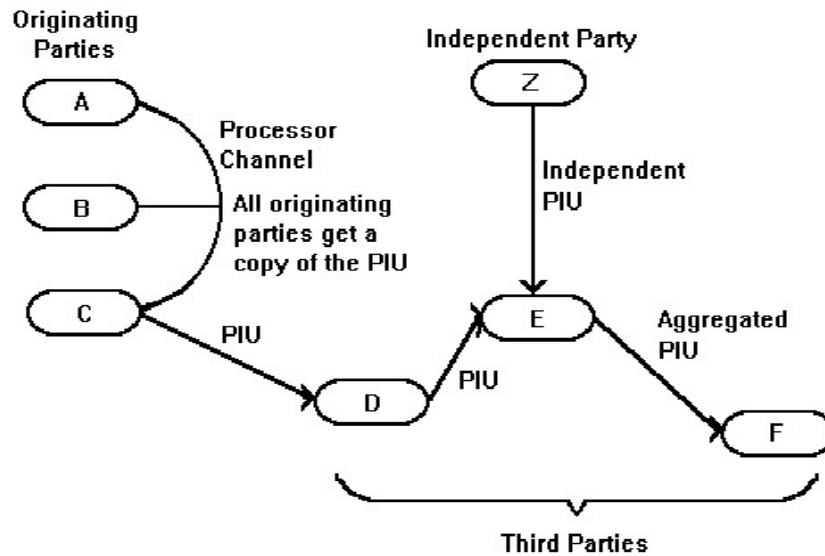


Figure A.3 A model of how a PIU is generated and how it may be transferred

The ease of access should not improve upon the acceptable access latency. Eventually vault storage may be all that is needed, but the ultimate in this respect is the eventual purposeful destruction of the AIU. Topology can aid with stationarity concerns by storing as much information with the client as is possible.

## A.5 Interfaces for Expanded Information Flow

### A.5.1 The HTIS as a Component of the PIE

The HTIS can operate in conjunction with the PIE. Information flow in the PIE is illustrated in Figure A.3. This model can include HTISs by substituting, where applicable, two vertices and the branch connecting them with the illustration in Figure A.4.

The concept of the PIU can be extended to operate within an HTIS to create an even greater degree of security. PIUs entering from outside the HTIS can contain IACLs which are relatively lax. The HTIS based on the principles of topology, aggregation, and stationarity could then factor an incoming PIU into AIUs protected as PIUs with more restrictive IACLs.

#### A.5.2 The Disk Pack Analogy

Topology, aggregation, and stationarity can be visualized by relating them to the physical configuration of a disk pack. A disk pack can figuratively be considered to hold all of the information (data items as well as processing functions) concerning a service offered to a particular client by an HTIS. Designing for stationarity separates the information on the disk pack into platters, designing for topology separates the information on the platter into tracks, and designing for aggregation separates the information on a track into sectors. A sector consists of an AIU. An access control list is formulated for each AIU and inclusion in an access control list is, as usual, determined on a need to know basis.

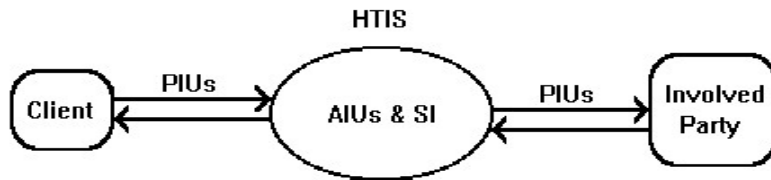


Figure A.4 Alteration to applicable branches of the previous model to allow for an HTIS.

There may be many services offered by HTISs where AIUs from different clients must meet. For instance, a bid and an offer price must meet to effect a trade. This can

happen in one of the rings of an HTIS if symmetry is approached -- similar sectors (AIUs) must be accessed. Some degree of symmetry is needed since if information availability deserves a certain level of restraint on one representational disk pack then generally the same should apply on another representational disk pack. Once information on a sector of another disk pack is accessed, this information becomes part of the accessing disk pack and it can travel to its inner rings. The alignment of sectors is illustrated in Figure A.5.

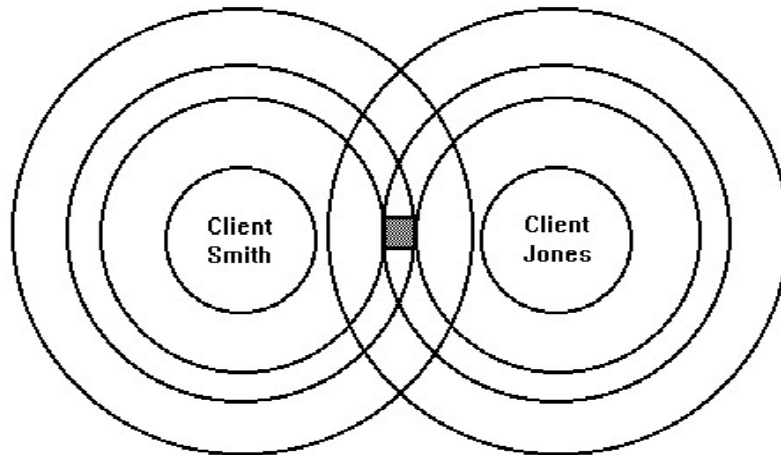


Figure A.5 Alignment of sectors of representational disk packs for two clients within the same or different HTISs.

By agreement between HTISs and their clients, different organizations can form standard representational disk packs. Transactions can occur among organizations, within HTIS tracks, by aligning sectors. Otherwise transactions can occur among organizations (if agreed to by their clients) within the involved parties track with sectors containing highly filtered AIUs. Just as PIUs can pass from information watchdog to

information watchdog, AIUs can pass from HTIS to HTIS through the alignment of representational disk packs.

The essence of this appendix is that an HTIS consists of different services and each service is treated as though it is offered solely for the benefit of a single client. The client is the center of a system, a representational disk pack, consisting of processing functions which are geared towards creating units of information, AIUs, to which tight fitting access control lists can be applied. Information can be exchanged among the representational disk packs of different clients, within an HTIS and across HTISs, as long as the level of access control is maintained.

The main part of this paper was largely concerned with systematizing the assignment of access control lists to information. The appendix was concerned with systematizing the formation of units of information so that tight fitting access control lists can be assigned.

## APPENDIX B

### THE INFORMATION PROTECTION TAG STRUCTURE

Abstract Syntax Notation One (ASN.1) will be used here to summarize the content of the IPT, as well as to offer a possible formatting approach. The level of ASN.1 notation needed for the communications recipient to uniquely identify each field, i.e., context specific tagging, will not be given since this level of detail may be more confusing than clarifying.

```
InformationProtectionTag ::= SEQUENCE{
    originators-link          OriginatorsLink,
    info-access-control       InfoAccessControl,
    identifying-info          IdentifyingInfo }
```

```
OriginatorsLink ::= SEQUENCE OF OriginatorInfo
```

The `piu-integrity-signature`, `audit-confidential-required`, and `audit-integrity-sig-required` fields in the following definition, and all the definitions which follow from these involve cryptographic data security techniques. These techniques are discussed in Chapter 3.

```
OriginatorInfo ::= SEQUENCE{
    piu-integrity-signature    ValidatingSignature OPTIONAL,
    originators-address        PresentationAddress OPTIONAL,
    alternate-address          PresentationAddress OPTIONAL,
    transaction-serial-number printableString OPTIONAL,
    origination-time-stamp     UTCTime OPTIONAL,
    audit-confidential-required Algorithm&PublicKey OPTIONAL,
```

```

audit-integrity-sig-required    BOOLEAN DEFAULT FALSE,
nonconfidentiality-allowed     BOOLEAN DEFAULT TRUE }

ValidatingSignature ::= SEQUENCE{
signature                       BIT STRING,
certificating-signature        CertificatingSignature }

CertificatingSignature ::= SEQUENCE{
signature                       BIT STRING,
validating-sig-verification    SignatureVerification,
validating-device-id           OCTET STRING,
validating-authority-code      OCTET STRING,
validity                       Validity,
certificating-sig-verification SignatureVerification,
certificating-device-id        OCTET STRING,
certificating-sequence-no      BIT STRING }

SignatureVerification ::= CHOICE{
signature-id                    SignatureID,
signature-cryptomethods        SignatureCryptomethods }

SignatureID ::= OCTET STRING

SignatureCryptomethods ::= SEQUENCE{
hash-function-identifier        HashFunctionIdentifier,
algorithm-and-public-key        Algorithm&PublicKey }

Algorithm&PublicKey ::= SEQUENCE{
algorithm-identifier            AlgorithmIdentifier,
public-key                     BIT STRING }

AlgorithmIdentifier ::= SEQUENCE{
algorithm                       OCTET STRING,
parameters                     ANY DEFINED BY algorithm OPTIONAL }

```



HashFunctionIdentifier ::= SEQUENCE{  
    hash-function                    OCTET STRING,  
    parameters                    ANY DEFINED BY hash-function OPTIONAL }

Validity ::= SEQUENCE{  
    notBefore                    UTCTime,  
    notAfter                    UTCTime }

PresentationAddress ::= SEQUENCE{  
    pSelector                    OCTET STRING OPTIONAL,  
    sSelector                    OCTET STRING OPTIONAL,  
    tSelector                    OCTET STRING OPTIONAL,  
    nAddress                    SET SIZE(1..MAX) OF OCTET STRING }

InfoAccessControl ::= SET OF AggregatedUsageState | { }

A null value ( { } ) for the IACL (InfoAccessControl) signifies that the information can be distributed to all recipients. The information watchdog does not allow the formation of a PIU which can not be accessed by any recipient.

AggregatedUsageState ::= SET OF AggregatedUsageInfluence

AggregatedUsageInfluence ::= SEQUENCE{  
    usage-grouping-code            BIT STRING,  
    naming-list                    NamingList,  
    control-attribute-list          ControlAttributeList,  
    nonconfidentiality-allowed      BOOLEAN DEFAULT TRUE }

NamingList ::= CHOICE{  
    concatenated-code-list          ConcatenatedCodeList,  
    range-list                    RangeList }

ConcatenatedCodeList ::= SET OF ConcatenatedCode

ConcatenatedCode ::= SEQUENCE OF EntryCode

EntryCode ::= BIT STRING

RangeList ::= SET OF Range

Range ::= SEQUENCE{

starting-parameter                    BIT STRING,

ending-parameter                    BIT STRING }

ControlAttributeList ::= SET OF AttributeValueAssertion | { }

AttributeValueAssertion ::= SEQUENCE{

attribute-type                    OCTET STRING,

attribute-value                    ANY DEFINED BY attribute-type }

For the "audit message" attribute-type and the "transfer approval" attribute-type, the attribute-value is a SET OF OCTET STRING which indicates the positions in the OriginatorsLink list of those originators that want to use these features.

IdentifyingInfo ::= SET OF OfficialSubject | { }

OfficialSubject ::= SEQUENCE{

key-word                    printableString,

nonconfidentiality-allowed            BOOLEAN DEFAULT TRUE }

## REFERENCES

- [1] The International Telegraph and Telephone Consultative Committee (CCITT), Blue Book, IXth Plenary Assembly, Recommendation X.500: "The Directory - Overview of Concepts, Models and Services," November 1988.
- [2] The International Telegraph and Telephone Consultative Committee (CCITT), Blue Book, IXth Plenary Assembly, Recommendation X.208: "Specification of Abstract Syntax Notation One (ASN.1)," November 1988.
- [3] The International Telegraph and Telephone Consultative Committee (CCITT), Blue Book, IXth Plenary Assembly, Recommendation X.209: "Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)," November 1988.
- [4] The International Telegraph and Telephone Consultative Committee (CCITT), Blue Book, IXth Plenary Assembly, Recommendation X.501: "The Directory - Models," November 1988.
- [5] Diffie, Whitfield and Martin E. Hellman. "New Directions in Cryptography." IEEE Transactions on Information Theory, vol. IT-22, no. 6, November 1976.
- [6] Needham, Roger M. and Michael D. Schroeder. "Using Encryption for Authentication in Large Networks of Computers." Communications of the ACM, vol. 21, no. 12, December 1978.
- [7] The International Telegraph and Telephone Consultative Committee (CCITT), Blue Book, IXth Plenary Assembly, Recommendation X.509: "The Directory - Authentication Framework," November 1988.
- [8] Madnick, Stuart E., and John J. Donovan. Operating Systems. New York: McGraw-Hill, 1974.
- [9] Dijkstra, Edsger W. "The Structure of the "THE"-Multiprogramming System." Communications of the ACM, vol. 11, no. 5, May 1968.
- [10] Schroeder, Michael D. and Jerome H. Saltzer. "A Hardware Architecture for Implementing Protection Rings." Communications of the ACM, vol. 15, no. 3, March 1972.
- [11] Voydock, Victor L. and Stephen T. Kent. "Security Mechanisms in High-Level Network Protocols." Computing Surveys, vol. 15, no. 2, June 1983.

- [12] The International Telegraph and Telephone Consultative Committee (CCITT), Blue Book, Ixth Plenary Assembly, Recommendation X.400: "Message Handling System and Service Overview," November 1988.
- [13] The International Telegraph and Telephone Consultative Committee (CCITT), Blue Book, Ixth Plenary Assembly, Recommendation X.413: "Message Handling Systems: Message Store: Abstract Service Definition," November 1988.
- [14] Tanenbaum, Andrew S. Computer Networks, 2nd Edition. Englewood Cliffs, New Jersey: Prentice Hall, 1988.
- [15] The International Telegraph and Telephone Consultative Committee (CCITT), Blue Book, Ixth Plenary Assembly, Recommendation X.200: "Reference Model of Open Systems Interconnection for CCITT Applications," November 1988.
- [16] Gasser, Morrie. Building a Secure Computer System. New York: Van Nostrand Reinhold, 1988.
- [17] Peyret, Patrice, Gilles Lisimaque and T. Y. Chua. "Smart Cards Provide Very High Security and Flexibility in Subscribers Management." IEEE Transactions on Consumer Electronics, vol. 36, no. 3, August 1990.
- [18] The International Telegraph and Telephone Consultative Committee (CCITT), Blue Book, IXth Plenary Assembly, Recommendation X.402: "Message Handling Systems: Overall Architecture," November 1988.
- [19] U.S. Department of Defense. National Computer Security Center. Department of Defense Trusted Computer System Evaluation Criteria. DoD 5200.28-STD. Fort Meade, MD: Office of Standards and Products, 1985.