Privacy, Security and Risk Management Considerations
Development of an SIV module

Q: What do we need to do to take privacy, security and risk management into consideration when we develop an SIV module?

A: Incorporate Security and Privacy within your Development Model
For example - Security Software Development Lifecycle

– Requirements
  • Identify policy, standards and procedures for methodology and built-in security features
  • Identify organization requirements/policy and outside regulations
  • Develop CIA goals and objectives
  • Perform risk assessment (business and technical)
    – Risk, likelihood, impact and cost

– Process – include security early in the cycle and continue through end
  • Threat Modeling
  • Security Design and architecture review
  • Secure Code Development
  • Security Code and peer review
  • Quality assurance and testing
Q: What are the five most important things needed to make an SIV application secure?

A: Consider that SIV applications are subject to many security breaches

- Inadequate data protection in transit or at rest
- Insecure software design, development and deployment (3rd party or in-house)
- Poor configuration of software security controls
- Wireless and physical security compromises
- Low defense – lack of layered security (applications, hosts and the perimeter)

Consider that the new VXML 3.x SIV environment is more complex and subject to more vulnerabilities

- Driving factors
  - Multi-modal input
  - Open source smart phones
  - Multiple networks
  - Multiple applications
Q: What are the five most important things needed to make an SIV application secure?

A: 5 minimal set of security tasks regardless of type of development lifecycle
   – Step 1: Envision - Identify Threats/Risks
   – Step 2: Plan - Profile, threat/risk modeling, generate requirements
   – Step 3: Develop - Control Check
   – Step 4: Release - Handle threat/Risk
   – Step 5: Stabilize - Learn and Educate

Recommendations to the industry to foster secure SIV software design, development & deployment
   – Subject SIV’s Design & Reference Implementation Code to Security Review
     • Use tools and experts – e.g. NIST competition for SHA-3 algorithm design
   – Devise attack plans and address vulnerabilities
   – Develop and/or tailor code analysis tools
     • VXML 3.x and SIV, initial and evolving implementations
Voice Models

Q: How keep my Database of voice models secure?

A: Utilize Standard Methods and Best Practices which are consistent with the organization’s security framework
  – Encryption, Hash
  – Access Controls
  – Policies and Procedures

Q: How keep my voice models and other data secure when I transmit them to others?

A: Utilize Standard Methods and Best Practices which are consistent with the organization’s security framework
  – SSL, VPN, Secure SOAP
  – Access Controls
  – Policies and Procedures
SIV Module Structure for Governance

Q: How can we structure the SIV module so that it can be governed by security and privacy policies of an organization?

A: Structure the SIV module to support proposed SIV framework

  - Management
    - Biometrics Policy (BP)
    - Biometric Practice Statement (BPS)
    - Event Journal
  - Security Infrastructure
    - Architecture, Techniques, Attacks, Risk Analysis
  - Environmental Controls
    - Biometrics Life Cycle
Security and Privacy Regulations

Q: What are security and privacy regulations of which we must be cognizant?
A: MANY and expect more

- **US** – Increasing Number
  - SOX – controls on sensitive data and assets of public cos.
  - GLBA – protect consumers financial information
  - HIPPA – Protection of personal health information
  - PCI – credit card transaction protection
  - FISMA – data security management requirements for federal orgs.
  - State by state disclosure regulations – big fines and big embarrassment
- **EU**
  - EU Directive – Protection of Personal Data
  - Basell II
- **Canada** - Personal Information Protection and Electronic Documents Act
- **Each country has their own set of regulations and cultural differences**
  - J-SOX
  - India’s Information Technology Act – cyber security
Q: Does SIV need a security framework?
A: Yes – SIV should exist within a security framework that facilitates:
   – consistent, comprehensive security
   – integration with other frameworks

Q: If so, what should it look like?
A: Multiple Security Frameworks are needed
   – Establish a security framework specific to SIV. Collection includes:
     • SIV framework documentation
     • Code analysis tools
     • Sample secure implementation code
     • DEFF (raw data) and tools – work underway
   – Establish a security framework for new set of VoiceXML 3.x standards
Security Summary

• Importance of the security development lifecycle
• Need for SIV Security Framework

References
• ISC(2) Security White Papers by Mano Paul, CISSP, MCAD, MCSD, Network+, ECSA
  – Software Assurance: A Kaleidoscope of Perspectives
  – The Need for Secure Software
  – Software Security: Being Secure in an Insecure World
• SIV Introduction and Best Practices Document, VoiceXML Forum