Secure Internet Letterhead.

Phillip Hallam-Baker,

Principal Scientist, VeriSign Inc.

Abstract

Internet crime dramatically illustrates the need to improve the security of the Internet infrastructure. New security infrastructures are needed to present Internet users with the information they need to protect themselves in a transparent and intuitive manner. For such a system to be successful it must be deployed ubiquitously and must therefore be an open infrastructure built on open standards.

Secure Internet Letterhead is an open technology built on existing standards that bridges the 'authentication gap' between the Web browser and the Web user establishing the identity of a trusted enterprise on the Internet using the same cue that is used in physical transactions – their trusted brand.

Security for Human Ends

The phenomenon of phishing illustrates two major flaws in the authentication mechanisms employed by Internet applications:

- The access credentials employed by the majority of Internet applications to authenticate users are insecure.
- It is too easy for criminals to impersonate a trusted party on the Internet.

The archetypal phishing attack is a form of social engineering. The target receives an email message that purports to come from their bank that requires them to disclose their account username and password.

The success of the attack depends on the existence of both security vulnerabilities. If it was not possible for the attacker to use a stolen access credential the attack would fail. If it was not possible for the attacker to impersonate the emails and Web site of the bank the attack would fail.

Strong Authentication Credentials

One solution to the particular problem of access credential theft is to replace password authentication with access credentials that resist or prevent appropriation by a third party such as One Time Password (OTP) Tokens and PKI Tokens (Smartcards). Credit card issuers in Europe have already begun a transition to using smartcards 'chip and PIN' for credit card transactions and many financial services providers in the US have already begun issuing OTP tokens to selected customers.

While deployment of strong credentials is important the problem of Internet crime is not limited to theft of Internet credentials. The credentials most commonly targeted in phishing attacks are credit card account numbers. Deployment of strong authentication credentials is an important goal in its own right but one that is already being adequately addressed by existing standards and ongoing standards activities. This is not the area where W3C can add most value at the current time.

Accountability based Security

Civilization was invented as a response to the need to security. The great cities of the ancient world were ringed with city walls to protect the city from external threat. The cities most precious assets would be held in a closely guarded treasury, a fort within a fort.

Early approaches to information security adopted a similar approach. The confidentiality and integrity of important information assets was protected by means of an access control mechanism built into the operating system.

Access control lists provide an effective means of protecting a closely controlled, valuable asset against a well defined threat. Like the ancient guarded citadels the access control approach provides a very high degree of security within a very limited area. The city walls could protect the assets of the craftsmen and merchants living inside them and the lives of any peasants who might be taking temporary refuge within but there was no way to protect the peasant's fields and houses without stretching the protective boundary so thin that all security was lost.

Security is achieved in social systems through varying degrees of accountability. A merchant who supplies shoddy goods will quickly gain a bad reputation and customers would go elsewhere. A complaint might lead to disciplinary action by the guild possibly leading to a reprimand or in extreme cases expulsion from the guild and loss of livelihood. A particularly aggrieved customer who failed to receive satisfaction from the guild might bring a lawsuit against the merchant. If the merchant's

conduct broke the law a criminal prosecution might be made.

The progress of civilization is the progress of accountability. Democratic government completes the accountability circle by making government accountable to the people.

The early Internet did not have cryptographic security controls built into the infrastructure. Despite this apparent lack the early Internet had strong accountability mechanisms as a result was exceptionally secure in practice. Access to the network was understood to be a closely guarded privilege, not a right. Misconduct of any kind would put that access in jeopardy.

As the Internet grew the accountability mechanisms that had kept it secure in its early stages were stretched beyond their capacity and failed. To secure the Internet we must restore accountability.

Secure Internet Letterhead

Current Internet infrastructure makes it possible for an attacker to effectively impersonate any other party they choose. The authentication mechanisms for email in particular are so poor that in some cases even an expert cannot determine whether a message is genuine or a carefully constructed forgery.

Public Key cryptography is a flexible and robust technology that is used to secure millions of Internet transactions each day. Like every technology it is also subject to important limitations of scope. In particular Public Key cryptography is by itself a technology for authentication of information and information machines. Public key cryptography does not by itself provide an authentication technology for people or organizations.

Public Key cryptography makes it possible to establish a near-infallible proof that a party to a communication used a computer system that had access to the secret component of a public key pair. The glue that is used to extend this technical authentication of machines to create a social mechanism for authentication of people and organizations is Public Key Infrastructure, in particular Trusted Third Parties also known as Certificate Authorities that issue digital certificates which assert the holdership of a public key pair by an identified subject that has met a specified authentication process.

The processes involved in managing the lifecycle of a digital certificate and criteria by which relying parties can estimate the trustworthiness of an issued certificate have been examined at enormous length. The question how a non-expert human user might interpret the information provided has been given considerably less attention than it requires.

Limitations of the SSL User Experience

The most successful public key security protocol deployed to date is SSL, subsequently adopted by the IETF as TLS. The SSL protocol is used to secure millions of Internet transactions worth several billion dollars each day.

Despite the considerable success of SSL in enabling Internet credit card payments the protocol is now 14 years old and has found applications far beyond the originally intended scope of use. Over the same time the community of Web users has expanded from approximately a million users mostly engaged in academic research to over a billion users whose primary uses are recreation and shopping. While the cryptographic component of the protocol has undergone substantial revision during that time to close certain cryptanalytic security vulnerabilities the SSL user experience is essentially unchanged since the original SSL 1.0 design. It should not be surprising therefore that the SSL user experience fails to meet current security needs.

A user experience can fail by providing too little information or by providing too much. The SSL user experience fails in both ways. For clarity we consider only the Internet Explorer user experience but identical flaws are present in all the major browser applications.

The first level of the SSL user experience is a padlock item that appears on a page that was received over an encrypted channel. As described below this provides the use with too little information.

The second level of the SSL interface is activated by clicking on the padlock icon. This is itself problematic as the padlock icon is not presented in a manner that would lead an ordinary user to click on it, nor would it help the typical user much to do so as interpreting the information provided requires a sophisticated knowledge of the X.509 certificate standard.

The Wrong Semantics

The presence of the padlock icon leads the user to believe that they are ‘safe’. This is unfortunately a false impression.

All the padlock icon actually means is that the communication was encrypted and the Web site visited was issued a certificate by an approved certification agency.

No Trust Differentiation

The SSL user interface was designed at a time when it was generally assumed that there would be a single provider of digital certificates which would enforce

authentication criteria that were generally agreed to be sufficient to ensure that certificates were trustworthy.

The VeriSign certificate subject authentication processes were drafted by lawyers working with security specialists. As such the designers of the processes were familiar with the principle of providing security by establishing accountability as accountability is one of the fundamental principles of law. The VeriSign Class 3 authentication process that governs issue of SSL certificates was designed to prevent credit card merchant fraud by ensuring that the certificate subject could be identified and apprehended should they be discovered to have defrauded a customer in some way.

The SSL padlock user experience provides no differentiation between authentication processes. The user is thus encouraged to trust a digital certificate even if the issuance process fails to establish subject accountability.

Caution is Penalized, Negligence Rewarded

The lack of differentiation in the SSL user interface has essentially precluded the introduction of more stringent authentication processes. Such processes do not offer value to certificate subjects unless Web users are aware that the subject has passed the more stringent requirements.

Relaxing the authentication criteria reduces the cost to the Certification Authority and reduces the burden on the customer. A pernicious cycle is established in which each new entrant into the certificate market offers a product that offers less protection to the consumer yet appears to provide the same level of trust.

What the user needs to know

User interfaces can fail because they provide too little information or too much. What is the correct level of information to provide to the user?

The best way to answer this question is to consider what the user needs to know in order to ensure that every party in the system is held accountable:

- In the case that the user is attempting to establish a new trust relationship with a party that they have only contacted online they need to know that if a default occurs, the certificate subject can be held accountable.
- In the case that the user has already established a trust relationship with a party the user needs to know that the certificate subject they are interacting with online is the same party that holds the offline identity.
- In order to ensure that the Trusted Third Party is held accountable the identity of the certificate issuer must be presented to the relying party.

Certificate LogoType Extension

Secure Internet Letterhead is realized by means of the PKIX X.509 Logotype extension[1].

The Logotype extension allows identification icons to be specified for the Certificate Issuer and Subject by means of a URL specifying a location from which the image may be obtained and a cryptographic digest of the image to allow authentication.

High Assurance Certificate Issue

Inclusion of certificate logotypes has the potential to create a security disaster if the issuance processes and certificate lifecyle maintenance processes allow attackers to fraudulently obtain certificates allowing them to impersonate the logo of a trusted brand.

Work on definition of criteria to ensure high assurance certificate issue is proceeding in other forums and should not be duplicated in W3C.

Application to Protocols

For maximum security to be achieved Secure Internet Letterhead should be used consistently and ubiquitously. Every form of electronic communication should be secured whether the medium is a document, a program, email, instant messaging or voice.

Although the long term goal is ubiquitous deployment this goal is best met in the short term by concentrating on the two killer applications for the Internet – Web browsing and email.

Of these applications the use of Secure Letterhead to HTTP transactions over SSL offers the best opportunity for completion of a standards effort in the short term. Paradoxically however the current state of flux created by the introduction of new authentication protocols, in particular DKIM means that application of secure letterhead to email offers the best near term opportunity for deployment, although standards ratification would be gated by completion of the DKIM specification.

User Centered User Authentication

As observed in the introduction the user authentication part of the problem is already being addressed in a large number of forums. It is neither desirable nor practical for the W3C to duplicate this work.

Where attention is needed is in the integration of these technologies into the Web infrastructure so that they meet the necessary level of usability to be employed by the general Internet user population and not confined to use within Intranet and Extranet applications.

In particular these technologies must integrate with two infrastructures that are core to the W3C mission – the concept of uniform identifiers and the HTML document format.

Uniform Name Space

The key advance of the World Wide Web was the introduction of a uniform identifier for information resources. A fully qualified URI allows any Internet user to identify the same information resource regardless of where they are accessing the resource from. The URI is unchanged even if the information resource is not accessible from a particular network location.

For user centered user authentication to be possible a user must have one of more network identifiers that are uniform: that is the *same network identifier* is used *regardless of the site* it is used at.

While such an identifier could in principle be established through the creation of a new global registry the Internet architecture dictates that the DNS be the sole federated namespace for the Internet.

The author believes that the only form of user identifier likely to be acceptable to typical users is an email.

Web Integration

Once a uniform namespace is established a variety of existing federated authentication schemes may be employed to authenticate the user against the user identifier claimed. SAML and the WS-* stack both provide an adequate infrastructure capable of extension to support arbitrary authentication schemes. HTTP Digest authentication with suitable modifications to support use in a federated environment might be employed to provide a secure means of accepting password based authentication in legacy Web browsers.

The principle missing component of such a system is a means of integrating the new federated authentication mechanisms into the Web infrastructure in such a way that a user who wishes to use a particular form of authentication need only obtain the necessary support from their identifier registry to perform the necessary authentication process.

For a Web site to authenticate a user's claim to a specified network identifier there must be means for that Web site to:

- Notify the Web client that the user is being asked to authenticate against the uniform namespace by means of a suitably specified HTML element.
- Notify the Web client of any nonce material required for the purpose of replay attack prevention.
- Determine which authentication service provider responds to authentication requests for the specified identifier.

Depending on the communication pattern required by the authentication mechanism the Web client may then either:

- Interpret the proof of authenticity provided by the Web client.

Or:

- Forward authentication data received from the user to the authentication service provider.
- Interpret the authentication decision from the authentication service provider

While the majority of this communication process is already defined in existing specifications the necessary HTML element is currently lacking.

Proposals

We propose that work to establish a mutual authentication capability for the Internet proceed on two separate tracks: Secure Letterhead and User Centered User Authentication.

These two tracks correspond to authentication in opposite directions, by the user to the Web site and of the Web site to the user. While authentication in both directions is essential if security is to be achieved the need for improved authentication of the Web site to the user is in need of most urgent attention.

Secure Letterhead: Web Sites

Gating Factors: None

Immediate progress can be made towards the specification of a technology platform and user experience principles for the use of Secure Letterhead for user centered authentication of Web sites.

RFC 3709 defines the technical means of embedding logotype information within an X.509 digital certificate. Currently a PROPOSED standard the specification is scheduled to progress to DRAFT standard in April 2006.

RFC 2560 (OCSP) defines the online certificate status protocol necessary to ensure that a logotype certificate is currently valid before display to the user, thus ensuring that the consequences of any failure in the certificate issue process can be contained and mitigated.

The principle issues that must be resolved to complete the specification of secure letterhead for this application are agreement on the principles that should guide a secure letterhead enabled user experience..

Secure Letterhead: Email

Gating Factor: Progress on Domain Keys Identified Mail Specification

Application of secure letterhead to email platforms is equally desirable to application to a Web environment. The main gating factor in this respect is the lack of a ubiquitously deployed *and used* domain level authentication infrastructure for email. While S/MIME supports end-to-end authentication of email the application of an S/MIME signature to a message changes the message content radically and prevents the message being read on a client that is not S/MIME enabled.

Domain Keys Identified Mail provides the ideal platform secure letterhead with the one proviso that development of the DKIM specification is currently being driven by an edge to edge use case and secure letterhead is intended for deployment at the endpoint of the network communication protocol in order to secure the 'final hop' from the screen to the user.

While applying secure letterhead DKIM does not require a substantial amount of engineering effort, the shift of focus from the incoming email edge server to the endpoint of the communication opens up additional opportunities that email client developers may wish to consider at the same time, in particular deployment of an encryption mechanism based on similar principles.

Secure Letterhead: Other Platforms

Gating Factor: Progress on Secure Letterhead for Web and Email

For secure letterhead to be fully effective the same security idiom should be used consistently across every form of communication. Every email, every Web site, every instant message and every telephone call should each bear the same consistent secure letterhead brand.

For secure letterhead to establish credibility and critical mass however the working group should first focus on the two 'killer applications' of the Internet – email and the Web.

User Authentication: Uniform Name Space

Gating Factor: Formation of consensus proposal

Although the past three months have shown considerable convergence amongst the competing 'Identity 2.0' proposals the situation is still fluid and no consensus architectural approach has yet emerged. While these efforts are close to the point where a formal standards effort may be beneficial there is still a risk that a premature attempt at standardization might lead to an unnecessary fragmentation of effort in multiple forums.

While the workshop may prove a catalyst for the necessary convergence of view the concepts are not thus far as advances as the secure letterhead concept. In any event, the goal of mutual authentication notwithstanding the requirements and technology involved in authenticating the Web site to the user are sufficiently different from those involved in authenticating the user to the Web site that the work should proceed in separate working groups in any case.

User Authentication: HTML Integration

Gating Factor: Uniform Namespace

Experience of HTTP Digest authentication demonstrates that for an authentication technology to be effective it must be integrated into the HTML document format.

The principle requirement for such integration is a HTML form element indicating that the user should authenticate themselves against the uniform name space. Progress in this area is thus gated on the establishment of the uniform name space.

Acknowledgements

This paper has greatly benefited from the work and insights of a large number of people. In particular Nico Popp, Siddharth Bajaj, Alex Deacon and Jeff Burstein at VeriSign

The Secure Letterhead concept was developed from concepts originally proposed by Stefan Santesson of Microsoft and refined by Amir Herzberg at Haifa University.

---

[1] **S. Santesson, R. Housley, T. Freeman**, *RFC 3709 - Internet X.509 Public Key Infrastructure: Logotypes in X.509 Certificates*, IETF, February 2004, http://www.ietf.org/rfc/rfc3709.txt