Financial Industry Requirements for Better Mutual Authentication

Chuck Wade (Chuck.Wade@FSTC.org)
Representing the members & participants of: Financial Services Technology Consortium (FSTC)
Better Mutual Authentication (BMA) Project (http://www.fstc.org)

ABSTRACT

Motivated by concerns that customer confidence in the online financial services channel is waning due to perceptions of vulnerability to fraud, FSTC's "Better Mutual Authentication" Project has convened a group of major financial institutions, industry associations, technology vendors, and government entities to examine the larger problem of authentication within the context of online retail financial services. This paper presents a few of the project participants' insights into the challenges of Web authentication and how to improve it; many of which have applicability beyond the financial services industry.

For additional information on FSTC's BMA Project, including additional related materials, see http://www.fstc.org/projects/bma-ph-1. Since this project is currently underway, relevant new documents will be posted prior to this W3C Workshop.

1 Introduction

Over the past decade, the financial industry and its retail customers have embraced the Internet and World Wide Web as a new channel for delivery of retail financial services, including payment transactions. The depth and breadth of financial services offered via the Web have expanded substantially in the new century, and a significant percentage of the world's retail financial business is now conducted via the Web.

The success of this Web-based channel has bred new problems, primarily in the form of new types of online fraud, online versions of traditional fraud, or offline fraud that leverages vulnerabilities in online services. So far, the financial industry has been remarkably effective at controlling this fraud,[1] but financial institutions cannot assume that current fraud-control measures will always be effective, and in any case the public visibility of fraud schemes such as phishing is eroding consumer confidence in the safety of on-line financial services, which troubles both financial institutions and their industry regulators.

One fundamental issue is authentication. Consumers are not as sure as they should be of the legitimacy of the Web sites they interact with, while the ability of financial institutions to authenticate their customers is being undermined by phishing schemes and other attacks aimed at stealing passwords and other sensitive information. The net effect is that people are losing confidence in the safety of conducting their financial business on the Web, which will have a negative impact on the growth and adoption of online financial services no matter how effective the financial industry is in controlling actual fraud losses. Government regulators, of course, are also concerned about this trend.

With these concerns in mind, the Financial Services Technology Consortium (FSTC) last year initiated a project aimed at defining "Better Mutual Authentication" practices for online delivery of retail financial services. This project has brought together major financial institutions from the banking and securities sectors, along with leading technology vendors, industry associations and observers from government agencies. New insights have emerged from this Project regarding the nature of authentication in a Web/Internet context, including the conviction that—although the necessary technology is largely available in theory—current Web authentication practices must be substantially improved if customer confidence is to be restored.

[1] Online fraud, by any measure, represents a small fraction of total fraud, and very few consumers suffer actual losses. Industry efforts at controlling fraud through backend detection and prevention systems have been very effective to date.

The project's position is that fundamental improvements cannot (and should not) be made by financial institutions acting on their own or through closed solutions. Ideally, the requirements of financial institutions and their customers would be incorporated into the specification of a web-oriented mutual authentication scheme that is broadly applicable to the many ways—including, but not limited to, financial transactions—in which people use the Web.

2 Position Statement

FSTC's BMA Project encourages and supports efforts by W3C to coordinate broad-based initiatives to improve Web authentication, and Project participants are likely to contribute to, or leverage, W3C's initiatives. From the FSTC BMA Project's perspective, requirements need to be addressed in the following eight areas:

1. Usability
2. Mutuality
3. Credibility[2]
4. Scalability
5. Availability
6. Interoperability
7. Flexibility
8. Adaptability

For financial services, the first three—*usability, mutuality,* and *credibility*—are the core requirements. *Usability* is vital. Embedded in the hardware, operating system, browser, and internet services available today in the average computer is a truly impressive array of security technology, but it's nearly impossible for the average consumer to make effective use of it, or even to determine if it is working correctly. Customer confidence in financial services can only be achieved if customers are able to confirm through trustworthy user interfaces that their Web interactions are safe.

At the same time, customer safety depends on protection from impostors who may attempt to impersonate either the customer to the financial service, or the financial service to the customer; hence, the need for *mutual authentication.*

Credibility[2] of authentication requires that both customer and financial institution confirm the authenticity of the other party using something better than just passwords or other shared secrets.

Beyond these core requirements, no authentication solution can be effective for retail financial services unless it can *scale* to support the entire consumer population. And consumers will resist adopting any new measures that impact *availability* of services, or that are too likely to break. Given the diversity of consumer needs, various authentication techniques will be required, and so *interoperability* is essential. Evolving consumer requirements indicate that *flexibility* is necessary to allow consumers to utilize multiple platforms in an anywhere, anytime online context. And, emerging threats and ever more sophisticated attacks from increasingly organized adversaries implies that viable solutions must be *adaptable* to a range of new threat scenarios.

Technology does not appear to be the issue. The current Web infrastructure, involving the Internet, Web server platforms and end-user platforms, provides vital security mechanisms that are widely deployed. Furthermore, there are many additional security techniques available today that can be used to augment Web authentication practices. However, inadequate controls, confusing user interfaces, inconsistent practices, and numerous vulnerabilities make it difficult to meet the authentication requirements of the financial industry.

The current state of Web authentication practices can be characterized as a confusing conglomeration of inconsistent techniques, often combined in *ad hoc* ways that result in ineffective systems that disempower both Web content providers and end users. Yet, financial institutions and their customers have found the Web to

[2] Rather than referring to "strength" or "security" of authentication, the term "credibility" is used to reflect the concept that authentication is really about how much confidence one party should place in the claims made by the other party, a much broader concept than, say, the mathematical strength of a particular algorithm or key length.

provide an appealing and useful foundation for an ever-broader array of financial service offerings. The dependency of financial services on the Web leads to a strong preference for improving Web authentication, as opposed to finding alternative channels.

FSTC's BMA Project participants recognize that the problems of Web authentication cannot be addressed by any one organization, or even by an entire industry acting alone. Instead, a coordinated approach is required involving:

- Operating System (OS) developers
- Providers of end-user computing platforms—*e.g.,* PCs, mobile devices
- Browser developers/vendors
- Web server software vendors
- Vendors of authentication techniques
- PKI service providers
- Web content providers—*e.g.,* financial institutions
- Internet Service Providers (ISPs)
- Standards-setting organizations
- Industry associations
- Government agencies
- End users—*e.g.,* consumers, citizens

W3C is well positioned to bring together many of these players to establish common objectives and align their respective strategies.

3 Financial Industry Recommendations

3.1 Reinforce TLS Mechanisms

TLS (and its SSL predecessor) represents a core capability of modern Web communications. While TLS is often viewed as a means for establishing a secure (encrypted) tunnel between a browser application and a Web server, it also provides authentication of the Web site via digital certificates issued by some Certification Authority (CA) hierarchy. If the client browser also has a suitable digital certificate, then the TLS session establishment protocol offers the ability to mutually authenticate both ends of the conversation—a much-needed capability.

Unfortunately, despite its considerable promise, practical use of TLS is hobbled by a variety of constraints and ineffective implementations that undermine its usability as a core security protocol. However, since TLS is a widely deployed, mature technology, the financial industry would like to see the problems corrected, and renewed commitments to shoring up the infrastructure to enable TLS to serve as a practical foundation for better Web authentication and safer web-based service offerings.

The most important requirements here are user interfaces that make it clear, in easy to understand terms, what the TLS infrastructure is doing.

The enhanced UI will go well beyond the existing locked padlock icon and display strong indicators that…

- The communication channel is "adequately" secured—*i.e.,* that the encryption technique and cipher strength meet policy guidelines.
- The site is who it claims to be—*i.e.,* the information presented by the site corresponds to identifying information contained within the site's certificate.

3.2 Leverage PKI More Effectively

Public Key Infrastructure (PKI) provides the means for issuing and managing digital certificates used in support of the TLS Web security discussed above and other security applications (*e.g.,* secure email, document signing, VPNs). Although PKI has a dubious reputation due to a variety of problems that hampered early

adoption, the fundamentals are sound. PKI services have continued to evolve, and digital certificates are now widely used in a variety of mission-critical and everyday business applications.

Once again, a key requirement lies in the area of user interfaces. For PKI to be effective in Web authentication, end users must be able to examine, install and manage certificates—both their own, and certificates associated with Web sites and Root CAs—without needing an education in cryptography or having to study X.509.

There is another issue associated with the plethora of Root CAs automatically accepted by most browsers. PKI alone, as currently implemented, does not allow a user to distinguish between a financial institution Web site and one that, although belonging to an impostor, has nevertheless obtained some sort of certificate and supports https sessions One possible approach would be for the financial industry to establish new guidelines for a restricted subset of the existing certification hierarchy that would issue certificates only to financial institutions, and then to add new indicators to the browser "chrome" that would let the user know whether a site's certificate is certified by this "strong" certification hierarchy.

Another attractive option associated with PKI is use of OCSP services to provide real-time validation of certificates. Consumers can use this capability today, though few understand what OCSP is, how it might benefit them, how to turn it on, or how to interpret what it is telling them. OCSP could also play an important role if certificates are issued to consumers. The financial industry would like to see OCSP broadly supported, and recognizes that financial institutions must also take steps to more effectively make use of OCSP.

3.3 Engage End Users in Mutual Authentication

Perhaps the greatest concern with current Web authentication practices is that end users—the customers of financial institutions—are severely handicapped in their ability to know if the Web site they are viewing is legitimate or an impostor. Although some evidence of site legitimacy is available to the user, particularly if the Web site has a certificate, the user interfaces provided for accessing and evaluating this evidence are obtuse and awkward to use. These problems must be resolved if consumers are going to have confidence in using web-based financial services.

It is also germane to note that there are inherent asymmetries when authentication must take place between human beings and machines—*i.e.,* user interfaces play an essential, integral role.

The financial industry would like to see new approaches to Web authentication that actively engage the user in authenticating Web sites (financial services) as well as providing stronger evidence of the user's authenticity. This will require active, two-way communications with users that provide consistent, understandable interfaces into the complete authentication process. However, user engagement should not become an additional burden or hurdle to be overcome. Instead, users should, at the very least, be given a *dashboard* they can trust and that provides the information they need when they need it, including useful alerts or warnings.

3.4 Achieve Synergies with Alternative Authentication Techniques

The financial industry recognizes that reliance on passwords alone is no longer adequate, given the current threat levels. Furthermore, the industry must address new regulatory guidance[3,4] that calls for use of alternative authentication techniques that protect consumers from password theft and abuse. Multi-factor authentication is widely viewed as one of the more effective alternatives available to financial services providers. However, there are significant challenges with rolling out new authentication techniques that will adequately scale up to the many millions of consumers that already use online financial services. In particular, consumer adoption is a major concern.

Once again, while the technology is available, the issues lie in deployment.

If alternative authentication techniques, such as multi-factor, are going to be accepted and used effectively by consumers, then they must play well with the computing platforms consumers are already familiar with,

[3] FFIEC recently issued new guidance on "Authentication in Internet Banking Environment" http://www.ffiec.gov/press/pr101205.htm

[4] "SEC Urges Investors to Protect Their Online Brokerage Accounts from Identity Thieves" http://www.sec.gov/news/press/2005-158.htm

including browsers and operating systems. The W3C is superbly positioned to promote a common way for alternative authentication techniques to be integrated into the existing Web infrastructure, through common architectural approaches and common interfaces.

In most cases, alternative authentication techniques will be used in conjunction with secure Web sessions based on TLS protocols, and may even be dependent on the prior establishment of secure sessions. Improvements made in the usability of Web security can be leveraged to help promote use and adoption of compatible alternative authentication techniques.

At the same time, there are new synergies that can be realized through better integration of Web authentication with alternative techniques. The financial industry seeks approaches that demonstrably improve security, enhance customer convenience, reduce problem rates, and lower the burden of customer support for all players, including consumers.

3.5 Improve Techniques for Managing Passwords

No matter what new authentication techniques get deployed, the financial industry will continue to utilize passwords and other shared secrets that can be exchanged bi-directionally between customers and Web sites. Browsers already provide password management tools for users, and increasingly serve as the preferred "password vault" for end users. Unfortunately, this concession to user convenience also heightens exposure to potential abuses, and financial institutions are increasingly concerned about the mounting threats to their financial services and customer interests.

Browsers also provide various means for end users to enter passwords through special-purpose dialogs, though all of these mechanisms are considered deficient in one way or another. The financial industry would like to see new password entry procedures incorporated into browsers that require prior establishment of TLS (SSL) sessions and that enforce effective security practices for use of passwords.[5] Financial institutions want more mechanisms for effectively controlling use of passwords—*not* to have browsers take control in ways that increase collective risks.

3.6 Security Policy Enforcement

Financial services providers have inadequate control over how browsers are configured when used to access sensitive financial information or high-risk transactions. It is even difficult for a Web site to ascertain how a particular browser is configured in terms of current security settings.

New procedures are needed that will allow financial services to stipulate that a browser's security configuration must meet minimum conditions, and to automatically upgrade (but never downgrade) any security settings that are deemed deficient. This will simplify security configuration for customers, yet allow financial institutions to set policies that provide adequate safety. Financial institutions would also like to have better options for determining if known vulnerabilities in a customer's browser or operating system have been corrected *before* allowing access to sensitive financial information or execution of high-risk transactions.

Acknowledgements

This paper represents the collective expertise and insights of the entire FSTC BMA Project. Many individuals have contributed to this paper, and helped develop the perspectives presented here. Project participants have also contributed to a substantial body of work that represents major contributions to the problems of Web authentication and related practices.

[5] For example, see *Stronger Password Authentication Using Browser Extensions* by Ross, Jackson, Miyake, Boneh, and Mitchell; http://crypto.stanford.edu/PwdHash