December 2006

Anti-Phishing Strong Authentication Technology Options

Paul Witman
Claremont Graduate University

Follow this and additional works at: http://aisel.aisnet.org/amcis2006

Recommended Citation
http://aisel.aisnet.org/amcis2006/131

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2006 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
Anti-Phishing Strong Authentication Technology Options

Paul D. Witman
Claremont Graduate University
paul.witman@cgu.edu

ABSTRACT
The United States banking industry has been directed by its regulatory agencies to provide authentication stronger than single factor for “high risk” transactions, as a defense against phishing. Financial institutions have a wide array of options available to them to meet this requirement, and choosing among those options is likely not a simple matter. Factors involved in the decision process include usability, security, and acceptability to the regulatory agencies. This paper presents an overview of the options available in the commercial market, and proposes future research to monitor the activities of financial institutions as they move toward the deadline.

Keywords
Phishing, strong authentication, financial institution, regulation.

INTRODUCTION
In October, 2005, in response to a growing volume of phishing attacks, the Federal Financial Institutions Examination Council (FFIEC)\(^1\) issued guidance directing US financial institutions to examine the risk profile of the functionality that they offered on the Internet, and ensure that appropriate measures were taken to protect customer privacy and data integrity, and to protect against online fraud (FFIEC, 2005). This guidance requires compliance by year-end 2006.

Phishing is defined as online attacks that attempt to extract confidential information from individuals. Numerous attack approaches are used to obtain this information. These include deceptive messages that convince a user to give out confidential information (delivered via e-mail or fax, in some cases), malware attacks that capture keystrokes or specific online banking credentials, DNS-based attacks that corrupt the mapping of domain names to IP addresses, and “man-in-the-middle” attacks that insert an attack server between the user and a legitimate web server (Emigh, 2005).

The FFIEC’s guidance emphasizes strengthening the authentication process for high-risk transactions. However, there is considerable latitude in the types of mechanisms that may be judged compliant with the guidance (FFIEC, 2005). Based on this guidance, it seems that most institutions are likely to choose solutions that result in stronger authentication of the end user.

Strong authentication solutions generally implement multi-factor authentication, requiring at least two of three fundamental types of proof of identity:

- Something you have (a physical device, a computer, a card)
- Something you know (a PIN code, the response to a challenge question)
- Something you are (a biometric such as a fingerprint or iris scan, or a behavioral metric such as a voiceprint) (Emigh, 2005)

The focus of this research is on the mechanisms available to financial institutions to comply with regulatory requirements for consumer services, and those requirements are due to be enforced by the end of 2006. Therefore, many citations are from the commercial space, studying options commercially available today or in the near future.

---

\(^1\) The FFIEC is an interagency body that prescribes principles and standards for regulatory agencies responsible for the regulation of the US banking industry. These include the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, the National Credit Union Administration, and the Federal Deposit Insurance Corporation (FFIEC, 2006).
Beyond these options, several researchers have published proposals for authentication of both users and servers. Topkara et al (2005) propose a shared-secret server authentication model to help prevent users from submitting their credentials to a fraudulent server. Jakobsson & Myers (2005) propose a new password protocol that delays exchange of password data until a stronger automated server authentication has been completed. Hiltgen et al propose a SmartCard and certificate-based strong authentication model called FINREAD that appears to be very strong, but carries the burden of a required distribution of media and hardware. A simpler variant of the FINREAD model has been adopted by at least one bank, Migrosbank in Switzerland (Hiltgen, Kramp, & Weigold, 2006). Few if any of these tools are yet evident in current commercial offerings.

Schneier (2005) further notes the limitations of two-factor authentication to defend against certain types of attacks. These include man-in-the-middle attacks, where the attacker passes the user’s credentials through to the real bank system, and Trojan or malware attacks that compromise the end user’s PC. Without additional defenses against these and future attacks, strong authentication is only a partial solution.

As financial institutions add stronger authentication to their online banking experience, they will need to ensure both usability and a sense of security for the end user. Tubin (2005) noted the need to strengthen authentication while maintaining customer convenience, or usability. Tan & Teo (2000) also found that security and perceived risk was a statistically significant, though weak, predictor of adoption among consumers in Singapore. Finally, Kolodinsky et al (2004) found a significant and positive relationship between the perceived safety and simplicity of PC banking with the adoption of this technology. This will affect both the choice of technology, and how that technology is ultimately marketed to the end users.

OVERVIEW OF COMMERCIALLY AVAILABLE TECHNOLOGIES

As might be expected, the imposition of a regulatory requirement has resulted in the offering of a wide array of alternative technologies to address the requirement. As with most security problems, a defense-in-depth solution is appropriate (Whitman & Mattord, 2003, p. 225). Such depth might include phishing detection tools (e.g., EarthLink, 2006), tools to assist the user to recognize a valid web site or valid e-mails (e.g., PassMark Security, 2005), and tools to strongly authenticate the user. Financial institutions could also deploy tools to track the creation of spoof web sites (Emigh, 2005, pp. 14-15), to take down such sites before they cause significant damage, and to monitor the launch of e-mail-based phishing attacks (Cyota, 2005b). The primary focus of this paper is on tools for strong authentication, ensuring against use of stolen credentials.

Several categories of strong authentication solutions have appeared in the market, including:

1. Hardware and software one-time password tokens,
2. SmartCards,
3. Non-electronic challenge-response tokens,
4. Risk-based challenge models,
5. Server-side software models, and
6. Client-server software models.

Each of these solutions provides different levels of ease of use and usefulness to the user, and varying levels of administrative costs to the institution. The vendors cited here often provide more than one solution option, and their appearance in a particular category is meant only as an example of one type of capability offered by that vendor. Figure 1 provides a context for how each of those solutions fits into the environment.

Software and Hardware One-Time Password Tokens and SmartCards

Hardware tokens are small electronic devices that generate a one-time passcode that can be validated by a server-side component, offered by vendors such as Vasco and RSA Security. The value of the passcode changes periodically, and is unique to each individual user. The passcode value is often appended to the user’s previously chosen password (e.g., E*Trade, 2005), and validated by the server at the time of login.

SmartCards are hardware devices that, when connected to the end user’s PC, can participate in the cryptographic exchange of credentials. The card may be embedded with a public key logon certificate, activated by a PIN code. This allows the card to serve as the “something you have” portion of a strong authentication sequence. (Smart Card Alliance, 2004)
The hardware-based model has the advantage of allowing the user to hold something tangible. This may provide a feeling of confidence that no one else can access the account as long as the user holds the SmartCard or token. (Wealth Management Bank, 2005). On the other hand, it has the disadvantage of a per-user cost for purchase and delivery of hardware, and the ongoing support costs to manage the devices over time, resolve issues, and replace broken or failed devices (Locher, 2006).

Software versions of hardware tokens are offered by some vendors, offering similar functionality to the hardware token but with the ability to use the software on a PC or on mobile computing devices such as cell phones and PDA’s (e.g., RSA Security, 2006). Figure 2 shows one vendor’s view of the architecture for authentication of users with one-time password tokens.

Figure 1. Strong Authentication Context Diagram

Figure 2. Token-based authentication (RSA Security, 2005)
Non-electronic Tokens

At least one vendor, Entrust, provides a token-based challenge-response security model that uses a non-electronic token. The token, often in the form factor of a credit-card sized plastic card, contains a table of rows and columns. The contents of the rows and columns are unique for each individual user. At login, the user is presented with a challenge asking for the content of certain cells from the table on the card, given a set of row and column information. The user is required to identify the correct cells and enter the data from those cells as part of the login sequence (Entrust, 2006). Figure 3 depicts the card and its use in the login sequence.

This shares the advantage, with the electronic devices above, of being a tangible item that the user can hold. It likewise shares the disadvantages of the need to deliver the items to users, and to replace lost or stolen items.

Risk-based challenge models

Several vendors, including Digital Resolve (2005), Quova (2006), and Cyota (2005a), offer a risk-driven authentication mechanism. Each of the models uses information known about the user’s behavior patterns along with information gleaned from Web (http) header and IP address information. Use of this information can provide insight into the physical location of the user, the type of browser used, the type of network connection used, etc.

Based on this information, if the user is found to be conducting transactions outside of their normal patterns of behavior, an additional challenge may be issued to the user. Such challenges may include one-time passcodes delivered via various media (cell phone, land-line phone, e-mail), or knowledge-based challenges for additional information previously agreed between the financial institution and the individual (Cyota, 2005a).

These solutions offer the advantage of simplicity for most users – as long as the user stays within their normal behavioral and geographic boundaries, no added challenges are issued. This may make the model vulnerable to a determined attacker who could spoof the various data elements required to fit the profile, and may also result in privacy concerns about the tracking of geolocation information (Berinato, 2006).

Server-side software-only models

Authentication models that do not require either software or hardware to be delivered to the end user may be perceived as being simpler for financial institutions to administer, and simpler for users to understand. These models are offered by many vendors, including PassMark Security (2006) and TriCipher, Inc. (2006). With this implementation, the user’s browser and a cookie or other browser mechanism serve together as the “something you have” component of the multi-factor authentication. Cryptographic software on the server ensures that a particular user can only log in from a PC and browser that contain the correct, current version of the secure cookie.

These solutions offer a lightweight implementation that may be well-suited to mass-market consumer adoption. However, this technique may be vulnerable to disruption by various mechanisms that might interfere with the storage of the secure data on the browser, such as explicit removal of cookies by the end user.

Client-Server software models

At least one vendor, TriCipher, Inc., offers the ability to use a downloaded software component as part of the cryptographic process of signing in to an account (Sandhu, Bellare, & Ganesan, 2002). This component interacts with a server-side component, to create a certificate that is used to authenticate the user and their PC via SSL client authentication. The user’s
password alone is not sufficient to log in from another PC, and the solution may be enhanced by storing part of the cryptographic material on a removable USB memory stick.

This solution is represented as providing protection against man-in-the-middle attacks (TriCipher Inc., 2006). However, it requires installation of software on the end user’s PC, and all the potential impacts that that entails.

CONCLUSION AND FUTURE RESEARCH DIRECTIONS

Many of these authentication technology vendors, responding to market forces calling for flexible and extensible solutions, have proposed integration of various of these technologies. For example, both TriCipher and PassMark have proposed integrating risk-based decisioning into their strong authentication frameworks. TriCipher has also proposed a rich set of capabilities including various combinations of cookie-based, software only, risk-based, hardware token, and biometrics functions (PassMark Security, 2006; TriCipher Inc., 2006).

Beyond the authentication technologies, the industry seems likely to be positioned to leverage single signon capabilities. Each service with high risk transactions that a financial institution exposes via the Internet may be subject to the FFIEC guidance (FFIEC, 2005). As such, a single user may be required to adopt multiple strong authentication technologies if a given financial institution does not require that all of its authentication requirements for that type of user be met via a single technology and identity management database. The Liberty Alliance has proposed a Web Services Framework for enabling identity management to span federated server networks. Users could then identify themselves at the “front door” of the institution, and have access to other authorized services without re-authenticating (Liberty Alliance, 2005).

Financial institutions will have to adopt strong authentication solutions that allow them to meet the regulatory requirements in a timely fashion. Those solutions must provide effective security to protect the institution’s customers and reputation, along with ease of use, to protect the end user experience and customer loyalty. Future research should be undertaken to assess the rate of institutional deployment of strong authentication solutions, along with measurements to assess the individual user adoption of, and satisfaction with, the technologies.

REFERENCES