passfaces™
STRONG AUTHENTICATION

A Phishing Story

Introduction

Reports of phishing attacks have inundated the press for good reason. The cleverness of social engineering has again damaged the prospects for online commerce, and online banking services in particular. Upcoming malware threats have added fuel to the fire. The stakes are high and remediation in the consumer environment, one that is fraught with unprotected clients, does not come easily. Without secure hardware in the entire authentication process, we must nod to the fact that absolute solutions to this problem are not currently possible.

However, with realistic risk assessment, it is possible to build a cost-effective, scalable solution. We must attack on all fronts. Although risk management tools other than authentication will be essential, the characteristics of the authentication mechanism used should add significant value to the overall countermeasure strategy. The user must be considered and the potential need for future changes must be recognized and built in from the beginning. The solution offered here is generic but Passfaces has some unique characteristics that allow for an innovative, effective solution that scales for consumer facing authentication needs and can be put into action now.

Definitions

For the purposes of this discussion, the following two attacks are key:

Phishing: A social engineering-based spoofing attack whereby a user is sent an email and spoofed into clicking on a link to a bogus website where personal information such as passwords and account numbers can be stolen. These can give the impression that the redirect is to the legitimate site (rather than a spoofed mock site) but in fact this is not the case.

Malware: Any executable code that is introduced to a computer without the owner's knowledge or permission with the intent of doing harm. These can be introduced through attachments to emails or visits to unknown websites where security vulnerabilities in Operating Systems, browsers, and web server software are exploited. Spyware and adware can be the vehicles for malware injection.

These two attacks may be combined.

Phishing by Social Engineering Alone

In the cleverest of these attacks to date, the user is sent an email, ostensibly from a financial institution with which the user has a trust relationship, warning him of the dangers and proliferation of identity theft. It further states that the link provided is an attempt by that institution to correct and remove some of the individual's risk in that regard. The text associated with the link looks like the URL of the genuine site; however the actual link is to a spoof website. When this link is followed, the spoofing website serves the user a web page that is a small pop-up box for the purpose of authentication; the bogus box floats over the "real" institutional site's authentication web page so that the user is not likely to suspect any thing abnormal. Even the fake URL has a name that seems legitimate in the context of the email as it includes words like "verify". This pop-up window in fact has no title bar to identify it, has an SSL padlock (that is only a .gif file), and displays words about using 128-bit encryption. Superficially it would be hard for even a skeptic doing a few checks to see the spoof. When the user enters his authentication data, the page sends the information back to the spoofing site. Phishing complete. The perpetrator has gained information that will allow him financial gain or access to information of value to him. The data collected is all usable without any expensive filtering or data mining techniques. The institution has no way to know directly that the spoof is occurring.

This type of attack is the latest in a long history of social engineering attacks. As Bruce Schneier is fond of saying, amateurs attack systems, professionals attack people. Its success is not dependent on any vulnerability in the end user's software. **People are part of any system they use and their vulnerability to social engineering is often the weakest link. Interfaces are always likely spots for intrusion but the one between man and machine is particularly susceptible because of basic incompatibility.**

Phishing with Malware

Malware, like screen scrapers and key loggers[1], require control over the target computer. Often malware relies on social engineering to accomplish this. This can take the form of email attachments that the user is tricked into executing or can be included with other software that the user is persuaded they want to download and execute (along with adware and spyware). Software exploits can also be used in conjunction with social engineering: the user is persuaded to follow an email link to a site that exploits a known vulnerability in order to introduce the malware. Accepting a license agreement alone can allow for the downloading and installation of malware. They are far more difficult to craft than a pure social engineering spoofing attack and take a lot more time to become effective, since they must first propagate themselves, install themselves and wait for the user to provide the correct trigger for activation. In addition, the filtering issue associated with malware is huge for the attacker. The data collected is not pure information when it is received. The attacker must sort through possibly megabytes of data to find the information being sought.

Given the complexity of the code in operating systems, browsers, web servers, and applications, it is not surprising that vulnerabilities exist. These vulnerabilities lead to worms, viruses, denial of service, and in this most recent case, to the acquiring of personal authentication information. Without processes in place (such as the Capability Maturity Modeling) during the development cycle for software, this situation is unlikely to be abated. Commercial pressures do not normally allow for the time commitment required by these processes.

Even with this caveat, discovering these vulnerabilities and making use of them has been limited mostly to benign worms that are more likely an expensive nuisance to clean up rather than a real threat leading to the long term loss of large sums of money. It is in the vendor community's interest to be watchful and make repairs where software vulnerabilities are identified. Blocking the offending IP address from the Internet is not easy to do and requires process and time to accomplish. But this can be, and is, done to eliminate the source in identified cases.

What Can (and Can't) Be Done?

- The solution to either of these attacks rests on setting and accepting at least three expectations:
- Absolute security is a myth; only relative security is achievable. This means that we layer our protection, make differential changes when they are cost effective, and thereby achieve an increased level of security (reduced level of fraud).
- No solution is permanent. Security is a process and planning for it to be a process is equally important.
- The cost of the solution path must be in line with the likelihood of loss through the vulnerability being addressed.

Given the nature of phishing attacks it is understandable that experts like Peter Tippett[2] say that the use of SSL and long complicated passwords (among other techniques) add little to the security profile[3] of a corporation or process. Employing these techniques just because they defend against known vulnerabilities fails to consider whether the REAL risks faced by a corporation are actually abated by these approaches. The key is to evaluate and weigh risk. What is the source of the real risk, the highest potential for harm and loss? For example today, social engineering risk far outweighs the risk of session interception in a switched network. This is part of the basis for Tippett's remarks above. Add to this that the SSL padlock can be attached to a fake web page in the form of a .gif file, quickly eroding the trust associated with SSL, as our initial example described.

---

[1] In reality, these are not usually attacks directly on the hardware (keyboard or screen) but rather focus on collecting data in Help Objects that do the data collection work needed for the legitimate request. Screen scrapes are more often recursive walks through windows to identify the one formatted to accept a password.

[2] CTO for TrueSecure Corp. Peter is considered to be the father of virus protection software.

[3] See http://infosecuritymagazine.techtarget.com/articles/june01/columns_executive_view.shtml

Countermeasures for malware attacks are difficult in an environment where the potential gain is high, coding is easy and positive control over the user's computer is impossible. These attacks remain less prevalent because social engineering is currently easier and more effective. However, where the potential gain is high enough, the necessary computing resources to inject malware and filter the resulting data can be justified.

The solutions to these attacks in a consumer environment are far more complex because cost, usability, reliability, and manageability weigh in differently than they do in smaller more highly controlled environments.

Solutions Objectives

Any user authentication discussion must acknowledge that in large consumer-based user groups the solution set is different because of cost, usability and manageability considerations. The strategy we propose here does not eliminate the consequences of phishing/pharming/malware attacks but reduces risk and fraud to more acceptable levels by taking steps to:

- Raise the bar for the attacker
  - More work
  - More time consuming
  - Reduced success rate
- Give the target institution a way to know an attack is underway
- Shorten the life of the attack
- Allow the user to be more actively involved in the solution but at the same time consider his ability to comply with any policy or remediation you implement
- Build a solution where the process can change without starting over.

Essential Enhancements to Web Authentication

Use two levels of user authentication: The first level provides limited authority (like viewing account balances, or moving money between accounts) while the second would be required for activities that culminated in the commitment of funds (such as authorizing payments or credit card charges). It is the user, not hardware loosely associated with the user that must be authenticated at both levels.

Make the second authentication session interactive: If the session requires user-specific information from the site, this raises the bar for the attacker. Generic attacks will not work. This also requires on-going contact to the real server by the attacker, which could provide the real site with the knowledge that an attack is taking place. Most importantly, the user is unable to complete the authentication process if the correct interactive information is not presented.

Increase user confidence that the site and the process are authentic: User specific data as part of the authentication process raises the bar on the difficulty of the attack and gives more assurance to the user that he is participating in a legitimate process. It also necessitates a second interaction by the attacker with the true site.

Create a random component to the authentication process: For the second level of authentication, do not require all of the secrets every time. Obviously this must be easy for the user in order to be reliable.

Plan for change in the process: Use an authentication process that minimizes the distribution of information and components to the customer community. Leaving the process in the control of the server allows for process change that is less costly.

Assure compatibility with other countermeasures: Reducing the risks of fraud and access theft will require more remediation than strong authentication. It is important that the authentication architecture chosen works well as a compliment to other components in the overall strategy.

Passfaces – The Solution Maker

The following ***seven countermeasures*** to phishing/malware concerns are provided by using Passfaces as the strong user authentication for online financial services.

Use two levels of user authentication: Passfaces is a cost effective, reliable strong authenticator to use for the initial site access or for the second level of access (along with a password for the first level). In fact, the risk profile changes dramatically if Passfaces is used initially. Because Passfaces are not socially vulnerable, the second factor can provide its own benefits rather than be implemented just to compensate for the weaknesses introduced by the use of a password. Passfaces requires no distribution of hardware, no custom software, and only minimal changes to any existing authentication architecture that currently accepts a password. It requires the user to perform no unfamiliar, often cumbersome, authentication tasks but rather leverages a natural talent that is familiar and present in all users regardless of age, education, or language. Customer feedback to date is overwhelming acceptance.

Make one of the authentication sessions interactive: Passfaces requires user configuration data to be presented before the authentication process can commence. Generic attacks will not work. Even in the event that a customized attack is developed, providing multiple face libraries randomly throughout the user population dramatically reduces the likelihood a given user will receive the face sets he needs to begin the authentication process. Divulging his secret is not in his control. When the user is unable to complete the authentication process, he will be eager to use any out-of-band reporting mechanism provided.

Increase user confidence that the site and the process are authentic: Some solutions rely on user education and awareness of the presence or absence of a user-chosen image to establish the authenticity of a site. Passfaces makes it impossible for the user to enter their authentication secret unless the correct library of faces is displayed, adding additional assurance that the user is at the correct site. Passfaces has enthusiastic user acceptance. Because the customer's participation is so active and easy for them, they have a heightened sense of confidence in the process.

Reliability and customer confidence are further enhanced by two factors. First, the grids are self-prompting; the user does not initiate the process. The customer cannot use his secret on more than one application unless the applications desire it. Secondly, the user is not asked to memorize or transcribe any numbers, letters, or symbols. His role is one he has been practicing since birth, i.e. recognizing familiar faces. Failure is rare for the legitimate owner of the Passfaces.

Raise the bar for keyloggers: Passfaces is not susceptible to today's keylogging attacks. By requiring the user to use a keypad in place of the mouse for image selection, both keystroke logging and screen scraping must be insinuated into the process and then the results must be combined and coordinated by the attacker in the harvesting phase. Because the image location changes with each session, the attacker must be prepared to identify the actual images before the secret can be used. This requires a much more sophisticated attack in both the harvesting and use of the secret, than is required where only passwords are employed (even one time passwords).

Create a random component to the authentication process: There is no limit to the number of faces that a person can retain. In a lifetime, the number is as large as it needs to be for any given individual. By being issued more Passfaces than are necessary for any single authentication, a subset of the faces can be randomly requested at each logon, thus eliminating the divulgence of the entire secret at any one time. This strategy might be followed for issuing Passfaces to high net worth customers. Once familiar to the user, Passfaces are reliably retained by the user for long periods of non-use, making this step possible.

Plan for change in the process: Because Passfaces requires no hardware distribution and no software installation on a customer's computer, changes in the process can be made as necessary from the server side. The client component can be modified and the presentation mechanism can be adapted to new requirements. As the phishing/malware attacks move on in complexity, Passfaces will stand strong in its essential service, requiring only modified implementations to keep it viable. See the companion paper, Implementation Security Strategies, for more details.

Assure compatibility with other countermeasures: Passfaces authenticates the user and so its focus is on the user interface. It is fully complimentary with other risk management solutions such as real time decision engines that assess the transaction environment in which the authentication in taking place. Passfaces can feed information to auditing and management tools and is compatible with existing backend databases. Our role in the risk management strategy is strong authentication of the user.

Passfaces will also be able to make use of future operating system enhancements such as those proposed by Microsoft as part of the Infocard system that will allow web-based user interface elements to populate their own private desktop and thereby restrict malware access to user-entered authentication data.

Conclusion

Consumer online transactions have requirements and constraints specific to that environment. With the growing sophistication of hackers, complete elimination/prevention of the effects of phishing and malware attacks is likely impossible, or at the very least, cost prohibitive. By taking a differential security approach, risk can be reduced by layering less costly approaches and thereby reducing the risk, not to zero, but to an acceptable level. By adding Passfaces as the strong authentication system, with its flexibility to raise the bar for the attackers in so many ways, the security posture of an online financial service offering can be increased by an impressive margin at a total cost of ownership that cannot be matched by any other solution.

About Passfaces

Passfaces, formerly Real User Corporation, is an information security technology company based in Annapolis, Maryland. The Company was founded in 2000 to commercialize an innovative, patented strong authentication technology that leverages the brain's innate cognitive ability to recognize human faces. Our Passfaces™ products offer business, financial services, government and OEM customers a cost effective, fully scalable and highly reliable strong authentication solution that supports business risk management objectives and is both liked and trusted by users. For additional information see: www.passfaces.com