Overview

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. However, with realistic risk assessment, it is possible to build a cost-effective, scalable solution. Although risk management tools other than authentication will be essential, the characteristics of the authentication mechanism used can add significant value to the countermeasures.

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 acceptable levels by taking steps to:

- Raise the bar for the attacker: more work, takes longer, 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 active 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

Passfaces – The Solution Maker

The following ***seven countermeasures*** to malware/phishing 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