Layered security in authentication. An effective defense against Phishing and Pharming

The most widely used authentication method is the username and password. The advantages in usability for users offered by *something you know* factors have historically compensated for the low level of security provided by passwords. This method can obviously only be used in low-risk scenarios and transactions but, in general, and we see this in practice, it is the access point to the biggest part of our day-to-day *digital life*.

Multiple attacks aim to steal the digital identities protected by the usernames and passwords. Of these multiple attacks, the most notorious and effective include phishing and its more sophisticated version, pharming. Basically, phishing attacks entail tricking users into believing they are connected to their genuine service providers' websites (their bank, the government, their email program, a social network, etc) so they enter their usernames and passwords in authentication processes that imitate the authentic websites'. The attacker obtains the usernames and passwords to use them illegally and impersonate the legitimate users.

The Anti-Phishing Working Group (APWG) releases on a regular basis statistics on phishing attacks around the world. In the first half of 2012[1], it identified 93,462 attacks aimed at 486 targets, including banks, e-commerce sites, government websites (especially related to finance and tax), online gaming sites and, increasingly often, social networks, ISPs and email providers.

How can we improve security while maintaining the usability provided by the username and password? And if a credential from another domain is used to access a service, which is occurring increasingly via our accounts for social networks and Internet and email providers? The solution is not always to replace the most popular authentication

[1] *R. Rasmussen, G. Aaron,* Global Phishing Survey: Trends and Domain Name Use in 1H2012*, Octubre 2012.*

method with a more secure one but rather to incorporate a layered security strategy and to add lines of defense to the authentication (defense in depth).

The Safelayer's new adaptive authentication solution implements a layered security strategy that starts with a first line of authentication based on the username and password. How it protects against phishing or pharming attacks illustrates how it works, although it also safeguards against other types of attacks, including offline cracking, online guessing, social engineering, eavesdropping, etc.

Website authentication

Phishing has a psychological dimension in that attackers take advantage of limitations in technical knowledge or lapses in good security practices to trick users. Measures against these social-engineering type attacks entail a prevention component aimed at warning the average user that something is wrong in the authentication process.

Phishing attacks are usually triggered when the user clicks on a link in an e-mail or Web page that takes the user to a false website. In general, users without a background in security find it very difficult to detect when they are being tricked into revealing their credentials. For this reason, it helps to use website authentication methods in which users can easily recognize whether the site they have connected to is authentic. If this authentication method worked in a way that was obvious to the average user, identity theft could be avoided on most occasions.

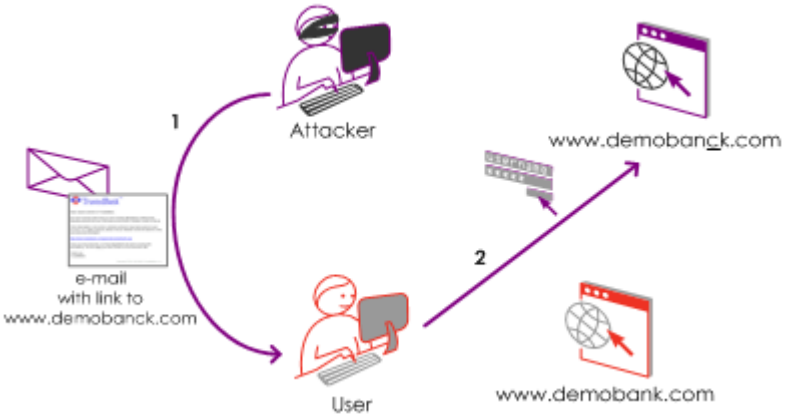

Figure: How a phishing attack works.

The most widely used Web server authentication method is based on the SSL/TLS protocol. The browser indicates that a website is authentic by displaying a padlock in the browser bar that tells users that they can trust the site and send sensitive data. However, a number of usability studies have found this method insufficient. For instance, the US Department of Homeland Security, Science and Technology Directorate (DHS S&T)[2] states that showing the padlock is not sufficiently effective for warning users not to trust a website

[2] A. *Emigh,* Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures (rev. 1.3)*, October 2005*

The article *Why Phishing Works*[3] estimates that 23% of users ignore the warning indicators in browser address and status bars, and that despite these indicators users make wrong security decisions 40% of the time. The study found that visual deception techniques are apparently effective even in the case of more advanced users and that the standard security indicators are not sufficiently effective for most users. It suggests that additional measures are required.

Owing to this need, Safelayer provides a solution in which users can select a personal image that is displayed in the form for entering credentials. Phishing protection derives from the fact that this image is different for each device (i.e., for each browser in an operating system account). So, even if a false website can exactly replicate the legitimate credential input form, it cannot replicate the customized image the user expects to see as this image is different for each user (and, in general, for each device used by each user).

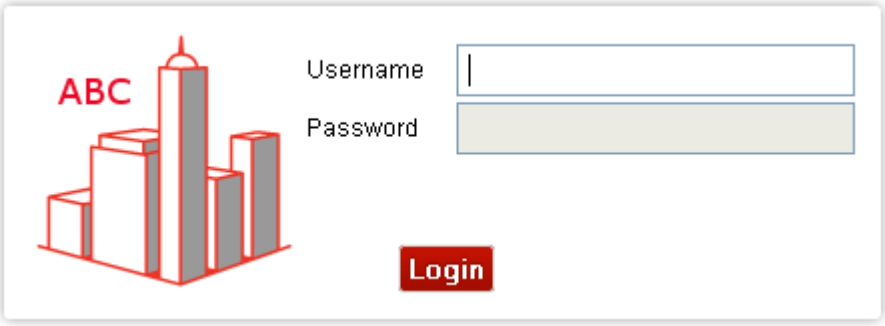

Figure: Personal image displayed in the form for entering credentials. The absence of this familiar image warns the user that the website is false.

The use experience of this type of solution based on a customized image is very straightforward. If users do not see the image they usually see and expect to see, they abandon the urge to enter their credentials and, therefore, the phishing attack is thwarted.

Device Identification

The solution described above allows associating a personal image to each device. For this to occur, the website requesting user authentication has to identify the device so that it can determine which image to display.

Furthermore, the advantages from being able to identify the device also improve the authentication service. Where an attacker manages to trick the user and steal the credentials and tries to use these credentials in a device different to the one the legitimate user normally uses, which the authentication service detects, an alert is launched and measures can be taken.

[3] *R. Dhamija, J.D. Tygar, M. Hearst,* Why Phishing Works, *Conference on Human Factors in Computing Systems, April 2006.*

According to the US Federal Financial Institutions Examination Council (FFIEC)[4], a distinction needs to made between:

- Simple device identification, in which a static cookie and/or an IP address are used to identify the device, and
- Complex device identification, in which one-time cookies are used and a digital fingerprint of the device is created that includes characteristics of the device such as information on its configuration, IP address, geolocation, etc.

The FFIEC states that although no authentication method is infallible, complex device identification is more secure and preferable to simple identification.

The key benefit of complex device authentication is the balance provided between cost, usability and security. The following table shows the levels of risk mitigation versus usability, financial and implementation costs compared to other methods.

Cost				Risk Mitigation			
Layer	Customer Burden	Financial Cost	Difficulty to Implement	Incident Occurrence	Financial Loss	Reputational Risk	Legal Exposure
Secure Browser Plug-in	Low - Moderate	Low - Moderate	Moderate - High	High	High	High	Moderate - High
Complex Device Authentication	Low - Moderate	Low - Moderado	Moderate - High	High	High	High	Moderate - High
Customized Images & Questions	Low	Moderate	Low - Moderate	Low - Moderate	Low - Moderate	Low - Moderate	Low - Moderate
Strong Passwords	Low - Moderate	Low	Low - Moderate	Moderate	Moderate	Moderate - High	High
Tokens	High	Moderate - High	High	Moderate	Moderate	Moderate	Moderate

Figure: Cost versus risk mitigation for different security methods (Source: American Bankers Association).

Safelayer's solution incorporates *complex device identifier* based management in which one-time cookies and fingerprints are used derived from multiple device parameters. The fingerprints identify the device's context (CDI), which includes the operating system and browser configuration (major and minor version; patches; sources; installed plug-ins; etc.), geolocation and time range.

The solution lets the user explicitly register one or more personal and trusted devices, i.e., as a *something you have* authentication factor. With this registration, users establish that these devices are always under their possession and control. Therefore, using them provides additional assurances on user identity. As a result, a lower risk of identity theft can be attributed to accesses performed with these devices compared to those performed with unregistered devices.

One-time Double-cookie Protocol

A cookie can be used to identify a device to display an image customized by the user. In this case, the cookie is sufficient for mitigating the risk of a simple phishing attack as the browser would never send a cookie to a domain different to the legitimate server's, in particular, the domain where the fraudulent server is located. Security is even further enhanced if the cookie's content is renewed in each authentication, making it a one-time cookie. This resource contributes to detecting the theft and fraudulent use of the cookie. For this reason, some solutions consider it enough.

[4] Supplement to Authentication in an Internet Banking Environment, *June 2011*.

However, in the event of an advanced phishing attack, i.e., a pharming attack, the attacker manages to divert traffic meant for the legitimate server to the fraudulent server. The attacker can then steal the cookie and, as a result, impersonate the device.

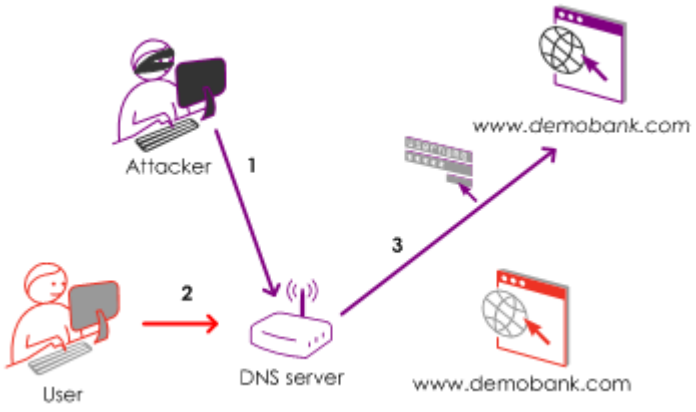

Figure: In an advanced phishing attack, i.e., a pharming attack, the attacker manages to make the browser believe that the fraudulent server belongs to the same domain as the cookie to remotely steal the browser's cookies. The figure shows how the attacker diverts the user to a fraudulent www.demobank.com site through prior manipulation of the DNS name system.

To combat pharming attacks, Safelayer's solution includes an additional layer of security through the use of what we have coined as the one-time double-cookie protocol, which uses a combination of two one-time cookies. These cookies have the following characteristics: They are marked as *secure* (i.e., they can only be sent by SSL) and as *http-only* so that they cannot be captured using JavaScript to mitigate cross-site scripting attacks. They have an expiration date and are associated to the client application's domain. Their content is a random value (i.e., they do not contain information on the user or the device) and is not generated from user or device variables. They are initially generated and sent the first time the user authenticates.

The first cookie (*Hello cookie*) is linked to the name of the legitimate server's domain and is still vulnerable to pharming attacks. The second cookie (*ID cookie*) is linked to a random path that is only known to the legitimate server that generated it. Thus, to identify the device, the server waits to receive two cookies according to the following protocol. Firstly, the *Hello cookie* is received. The server uses this cookie to identify the device, which it redirects to a page with the exclusive path to which the *ID cookie* is associated to, which only the legitimate server knows. If the browser finalizes the protocol and sends the *ID cookie*, the server can complete the identification of the device and, for example, display the customized image. This is how the mutual authentication process between the device and the server is carried out.

To minimize the possibility that the cookies may be used fraudulently if captured, the random value in the cookies is renewed each time the customized image is obtained (prior to authentication) and each time the user authenticates successfully. Users registering devices does not require making any changes to the cookie exchange protocol or content.

So, thanks to the one-time double cookie, fraudulent servers cannot cause the sending of the second cookie because they do not know the exclusive path to which it is associated and the pharming attack is aborted.

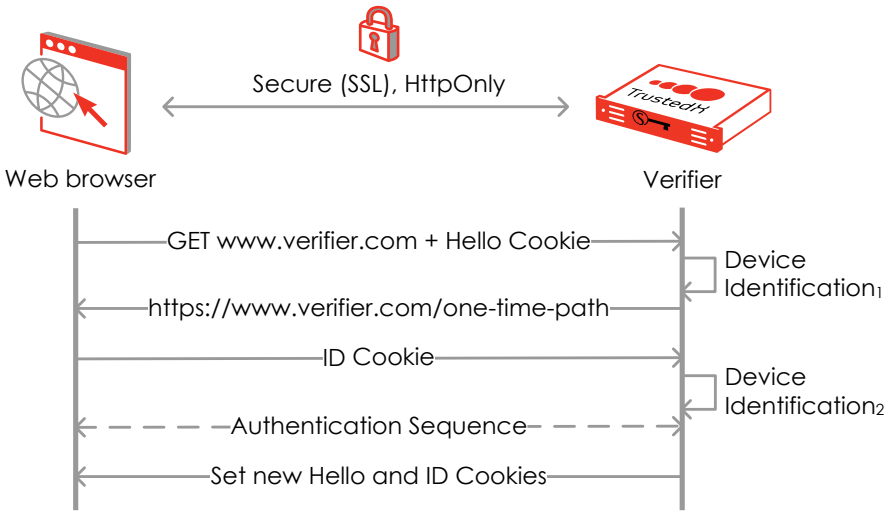

Figure: The one-time double-cookie protocol implemented by TrustedX.

Thanks to the incorporation of this new layer of security, Safelayer's solution improves upon the FFIEC's expectations for complex device identification and most other existing solutions based on one-time cookies.

Safelayer's Adaptive Authentication

Safelayer's adaptive authentication solution maximizes the level of security of the authentication using a layered approach (layered security) while reducing the costs of implementation and deployment and also, very importantly, the cost in terms of usability for the users.

The solution increases the security of the first line of authentication (based on username and password) through the introduction of additional measures including the display of a customized image and complex device identification through the one-time double-cookie protocol. Furthermore, it incorporates an engine for analyzing the user's context that allows assessing the risk of identity theft by correlating device, location, time and other parameters. Based on the results of this analysis, a second line of authentication may be executed, e.g., a unique code sent in an SMS message or email, a unique code generated in an OTP device or mobile app or, in general, any method that can be integrated into the system.

The context analysis can be complemented with a biometric system that recognizes the user's keystroke dynamics. This line of defense is transparently integrated in the form used to enter the username and password (or any other equivalent or additional field) so that the analysis engine can determine if the user that entered the credential is the legitimate user by comparing the typing pattern detected with that registered for the user. This method allows detecting if the user, voluntarily or otherwise, gave their credential to another user. This mitigates social engineering attacks.

A policy-based system can be used by the organization to tailor the security levels (first line, context risk analysis and second line) to the scenarios most suited to its security and cost requirements and to its users.

These authentication security layers must be complemented with others, especially ones related to i) education, control and the relationship with the users and ii) the intelligence

analysis. The first type raises user awareness about and commitment to good security practices, and the second strengthens decision-making in the authorization of high-risk accesses and transactions. In this respect, the information captured and generated in the authentication phase is of great value in terms of business intelligence. In short, it is always better to optimize usability and convenience on the user side and security and cost on the back-end side.