2011

Password-Based Authentication and Phishing

Edina Hatunic-Webster
Technological University Dublin

Fredrick Mtenzi
Technological University Dublin, fred.mtenzi@tudublin.ie

Brendan O'Shea
Technological University Dublin, brendan.oshea@tudublin.ie

Recommended Citation

Hatunic-Webster, E., Mtenzi, F. & O'Shea, B. (2011). Password-Based Authentication and Phishing. *eCrime Researchers Sync-Up*, University College Dublin's Centre for Cybercrime Investigation, March 15th and 16th.

Password-Based Authentication and Phishing (Extended Abstract)

Edina Hatunic-Webster, Fred Mtenzi, Brendan O'Shea
School of Computing
Dublin Institute of Technology
Dublin, Ireland
{edina.hatunic-webster, fredrick.mtenzi, brendan.oshea}@dit.ie

1 INTRODUCTION

The most common mechanism for online authentication is the username-password. Majority of e-commerce applications are designed to provide password authentication via an HTML form, with the assumption that the user needs to determine if it is safe to enter the password. In order to avoid phishing attacks, the user is expected to distinguish between a phishing and a genuine website by checking the browser security indicators.

Alternative authentication models suggest using images for authentication, introducing variations of Password Authenticated Key Exchange (PAKE) protocols into TLS, using digital objects as passwords. Some authentication models suggest sending one-time password (OTP) tokens out-of-band to the user.

Most computer users have too many passwords and keep forgetting them. Common issue for all authentication models is how to restore a legitimate user access to their account without authentication, i.e. password reset.

In this paper, we investigate current password based authentication models and review their impact on phishing. We investigate two categories of issues 1) deployment obstacles for the 'stronger' authentication models, and 2) security issues created by the number of passwords user needs to memorize.

The analysis of these models points to a conclusion that one authentication solution does not fit all problems. As technology increases and cost of hardware decreases, more authentication options should be examined and implemented. Strengthening both the user awareness and authentication to make it harder to steal and use credentials should alleviate the phishing problem.

2 PASSWORD AUTHENTICATION AND PHISHING

The username-password authentication dates back from the time when authentication was done from physically protected terminals that are assumed to be secure. As Internet security flaws were recognised, Secure Socket Layer (SSL) and the Transport Layer Security (TLS) protocol were added to protect e-commerce applications. SSL and TSL use Public Key Infrastructure (PKI) certificates to authenticate servers, i.e. websites, by installing trusted certificates on client's browsers. Most e-commerce financial institutions use these certificate and rely on trusted third parties to authenticate certificates (i.e.users) on their behalf. In spite of this, phishers succeed to take users into the spoofed websites. Unfortunately, SSL can not protect against web-based password theft used in a phishing attack as certificates can be acquired by any party including phishers.

The PAKE research explores an alternative approach to protect password without relying on a PKI. PAKE schemes only require that a human memorable secret password is shared between the participants. Using PAKE by itself does not protect against phishing, as keyloggers can record the password. Also, if PAKE is to be used for web authentication both server and client side need to be changed and must participate in the PAKE protocol.

Some of the PAKE anti-phishing protocols employ zero-knowledge authentication, which is a practical application of the concept of a zero-knowledge proof (ZKP). In a zero-knowledge proof, one party can confirm whether or not a statement is true without revealing any other property about the statement. Other combine it with SSL or TLS. The deployment problem with these scheme is a high computation cost.

Graphical passwords are generally easier to remember and use than complex alphanumeric passwords. Hence, graphical password systems have been suggested in various forms as an alternative to passwords. Images are used as way to successfully authenticate sites, by using a randomly generated visual hash to customize the browser window or web form elements to indicate the successfully authenticated sites. Images can be also used as a password recovery mechanism as humans can easier recognize images than recall a secret question set a some time in the past.

Graphical password systems also suffer from deployment related issues: e.g. how to secure storage and display of the secret image in browser; spyware and keyloggers - a phisher can intercept an image in the same way as a an alphanumeric password.

Two-factor authentication is deployed in various forms: as a chip and PIN; OTP tokens - devices that generate random passwords that is only valid for use once, hence limiting the the amount of damage even if the password is intercepted bu a phisher. Some authentication system can send OTP out-of-band to the user, for example as an SMS to the user's phone; or in the form of transaction numbers (TANs). One-time password are often valid for a limited, short time period, requiring a phisher to act immediately.

Two-factor authentication models require users to either carry token, smart cards and require more effort on behalf of the user and provision and maintenance of hardware by the service provider.

As the number of services and website increased, most computer users have a large collection of accounts with different applications. Good security practices recommend that users should be educated to choose high entropy passwords. In reality, users choose simple passwords, or pick the same or similar passwords they already use for different, higher-security applications. If the system forces them to choose a complex password, users usually write them down or forget them regularly. The large number of passwords increases the chance of users forgetting them. Questions normally used for password recovery (i.e. mother's maiden name, place of birth, or colour of eyes) are readily available on the Internet and are similar between websites of different security importance.

Most of the reviewed anti-phishing authentication models ignore the requirement of designing an authentication system that is able to cope with the fact that users periodically forget their passwords or loose the authentication token. Most of them rely on Email-based identification and authentication (EBIA) automatic password reset mechanism in spite of many security risks.

Some researchers suggest using images for as a password recovery mechanism. Also, systems where users are authenticated using their preferences is proposed as a password recovery mechanism is suggested.

There are many organisations (e.g. governments, financial institutions, universities) that can vouch for a user's identity and a specific set of attributes (age, citizenship, memberships, student enrollment status). These existing resources could be used as the 'fourth factor authentication' or as part of the initial authentication or forgotten password schemes.

3 CONCLUSION

The analysis of these models points to a conclusion that inadequate authentication mechanisms used by the banks, credit card systems and other Internet service providers is one of the main factors in success of phishing attacks. Until the direct economic losses become large enough, there may be little incentive for service providers to make changes that could lead to problems in support costs.

Problem is that authentication models that are both secure and usable can only be devised by combining shared secrets with other authentication technologies, such as biometrics, out-of-band signaling devices or specialized hardware. Stronger authentication models require users to either carry token, smart cards or generally require more effort on behalf of the user. And the users are also reluctant to do so.

As many studies concluded that users are not capable to figure out if they are phished or not, we should design authentication models in such a way that even if the user users credentials are phished - the damage is minimised/contained. Also, service providers should be encouraged to use authentication model that assumes that user can not distinguish between a phisher and a genuine website.