Protection Mechanisms Against Phishing Attacks

Klaus Plössl, Hannes Federrath, and Thomas Nowey

Universität Regensburg
{klaus.ploessl, hannes.federrath, thomas.nowey}@wiwi.uni-regensburg.de

Abstract. Approaches against Phishing can be classified into modifications of the traditional PIN/TAN-authentication on the one hand and approaches that try to reduce the probability of a scammer being successful without changing the existing PIN/TAN-method on the other hand. We present a new approach, based on challenge-response-authentication. Since our proposal does not require any new hardware on the client side, it can be implemented with little additional cost by financial institutions or other web retailers and therefore is a good compromise compared to the other approaches. A big drawback is that it doesn't protect against man-in-the-middle attacks but most of the other approaches don't either.

1 Introduction

Phishing – "the hottest, and most troubling, new scam on the Internet" [1] – is a relatively new fraud technique, utilizing methods of Social Engineering. The "victim", an online customer, is tricked into divulging personal data (e.g. passwords, credit card number or online banking account) to an attacker. In 1996 the term Phishing – a combination of "password" and "fishing" – was first mentioned on the internet in the alt.2600 hacker newsgroup. See [2] for further information.

The Anti-Phishing Working Group (APWG), an association of financial institutions, internet service providers, online-retailers, and other it-companies, is collecting information on Phishing incidents. The collected data is published in the monthly Phishing Activity Trends Report, which clearly shows the dramatical increase in Phishing attacks during the last few months (see Fig. 1). Another study conducted by Gartner showed that 57 million US citizens have already been victims of a Phishing attack. 1.4 million or 2.5 % of them passed sensitive data unknowingly to third parties which cost banks and credit card companies $ 1.2 billion in 2003 [4]. According to the APWG-data even 5 % of the attacked are supposed to become victims.

Timeline of a Phishing Attack. According to [5] there is a characteristic procedure:

1. In most cases the attack begins with an email that pretends to come from a reputable service provider like a bank. At the first glance the fraudulent

S. Katsikas, J. López, G. Pernul (Eds.): TrustBus 2005, LNCS 3592, pp. 20–29, 2005.

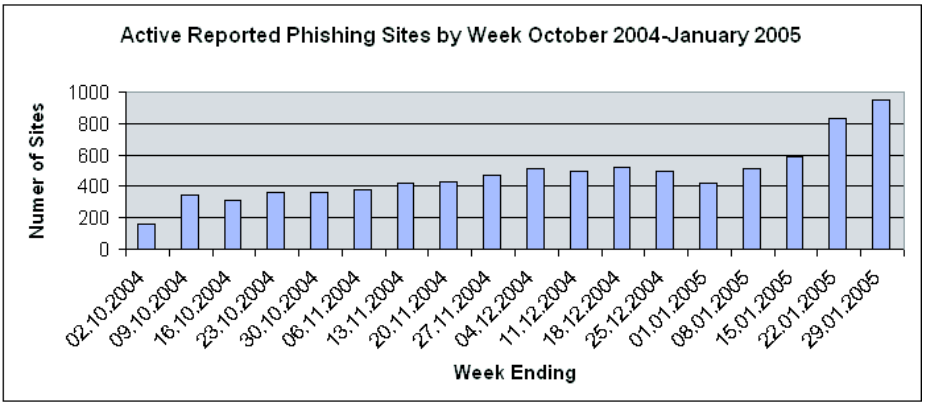

Fig. 1. Active Reported Phishing Sites by Week October 2004-January 2005 [3]

email looks reliable regarding its sender, form, and content and is thus almost indinstinguishable from a real one. Frequently a necessary update, a loss of data or even a security problem is the pretended reason for the mail.

2. With the email the victim is tricked in following a hyperlink to a counterfeited website. Like the initial email this website is hardly to identify as an imitation, because its look and feel is adapted to that of the original one. The target of the hyperlink within the email can easily be counterfeited using html-mails. There are several methods to disguise the address in the address-field of the browser, like:
   - Using a similar domain-name (e.g. https://www.postbank-deutschland.com instead of https://www.postbank.de)
   - Exploiting bugs in the browser software (e.g. using long addresses containing the @ character)
   - Using sophisticated methods like "Floating Windows" – small Java Script programs that overlap the original address-field of the browser (containing the address of the scammer's website) with another window containing the pretended address.
3. The faked website asks for personal data or access information from the user that is then used for fraudulent transactions.

The tricks and methods of the Phisher become technically more and more sophisticated what makes them also more dangerous for the victims. A recent example is a Phishing email containing scripting code that is used to manipulate the hosts-file of windows-machines [6]. Since this file is used for the resolution of domain-names the user is automatically redirected towards the attackers page when he enters the original URL of the service. It is noteworthy that with this type of attack the content of the fraudulent email does not necessarily have to have any relation to the later target, what makes the user even more careless. This type of attack is also known as "Pharming".

The remainder of the paper is organized as follows. First we present known countermeasures against Phishing (Sect. 2). We continue by proposing a new solution to the problem (Sect. 3) and finally we evaluate our approach and compare it to the existing ones.

2 Known Countermeasures

Meanwhile there are a lot of protection mechanisms against Phishing and online-scammers. These proposals can roughly be separated into two categories: modifications of the traditional authentication and authorisation-method (PIN/TAN) on the one hand (Sect. 2.2) and approaches that try to reduce the probability of a scammer being successful without changing the procedure on the other hand (Sect. 2.1).

2.1 Minimizing the Risks

This group can be divided into user-dependent and user-independent approaches.

User-Dependent Approaches. Most user-dependent approaches are based on a kind of guideline that is given to the users and contains information about the correct usage of the service. The complexity of those guidelines is varying heavily. Some examples are [5], [7], and [1]. The problem with these guidelines is that the average Internet user is likely not to put into practice all of those recommendations – either because he is not capable of doing so or for convenience reasons. Tools can support the user in terms of security.

Spam-Filters and Filters for Outgoing Data. Manufacturers of anti-virus software try to hamper Phishing by the use of filters. Already known Phishing mails and faked hyperlinks can be identified and the corresponding email can be classified as spam. Filtering Software is also capable of scanning the outgoing traffic for sensitive data, blocking it and immediately sending a notification to the user.

Browser Plug-Ins. Browser plug-ins like SpoofStick make it easy to verify the URL of the currently visited website. The plug-in-software shows the name of the currently displayed website in a user-configurable color and size (e.g. "You're on ebay.com"). This is an effective countermeasure against attacks aiming to confuse the user by modifying the address-bar.

The plug-ins ScamBlocker, TrustWatch and Phish Net all use blacklists with well-known Phishing-sites. Everytime the user wants to visit a website it is compared to the list and in case of a match a warning is displayed to the user. Additionally Phish Net prevents any kind of navigation through the elements of that site. The software also stores sensitive user data and issues a notification to the user every time such data should be transmitted via the Internet.

SpoofGuard visualizes its classification of a website by a traffic light (see Fig. 2) and if necessary a pop-up-window with a warning. The classification depends on various indicators that can be invidually assessed by the user. For further information see [8].

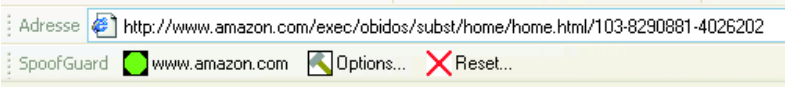

Fig. 2. SpoofGuard

Another tool from the developers of SpoofGuard is PwdHash, an Internet Explorer plug-in, that computes a hash value from the domain-name of the currently visited website and the password entered in the password field of the site. Instead of the password chosen by the user the hash value is transmitted to the website. Thus the "passwords" (read hashes) transmitted are different for all domains and a scammer will not get the right password for another domain by luring the user to a faked domain.

User-Independent Approaches. All tools mentioned above have to be installed manually by the user. The service provider has no influence on the (correct) usage of these security measures. In contrast the methods illustrated in the following can be implemented solely by the service provider.

Spam-Trap and Domain-Watch. Spam-Trap and Domain-Watch are two different approaches that aim on informing the service provider at an early stage of an attack. Then he is able to give a warning to his customers early enough to protect them.

- For Spam-Trap email-addresses are dropped in numerous newsgroups, guestbooks and websites with the goal to get as many spam-mails as possible to that addresses. The incoming emails are subsequently analyzed and if a new Phishing attack is identified the affected service provider is notified.
- Domain-Watch monitors the registration of new domain-names. Every time a domain with a name similar to that of an existing service provider is registered a notification is sent. By this means the service provider can prepare the suspension of that domain in case of an attack. According to [3], the time domains used for Phishing attacks were reachable and working, averages 5.8 days. By identifying the owner of that domain before the attack begins, the service provider is able to considerably shorten that time-period and may even be able to prevent the attack.

Meanwhile there are a couple of firms that monitor spam and domain-registrations for other firms (see [9]). They even offer countermeasures for the case of emergency that can go as far as denial-of-service attacks on identified Phishing sites.

Validation of Sender Information. Sender-validation-techniques are designed to identify spam and Phishing emails respectively to determine their real originator. According to [10] all currently available techniques are based on an extension of the mailserver-entries in the DNS.

Although there are several proposals for the technical realisation a common standard has not yet been realized. The IETF working group MARID (MTA AuthorizationRecords in DNS) announced its dissolution in September 2004, after a controversy over patent claims of Microsoft Corp. concerning the "Sender ID" method, which was the favoured method of the working group up to that point [11]. Now the different proposals are supposed to be submitted as individual RFC-drafts to the IETF.

Fraud Detection. Major enterprises normally have the ability to analyze all data for irregularities in real time. Such irregularities can usually be observed when a scammer tries to use information obtained by a phishing attack for a transaction. The Internet Payment Service PayPal uses a 24/7 fraud and spoof detection system, that is capable of identifying anomalous transactions within one hour. Each transaction is checked for plausibility (amount, frequency of usage, etc.) and can be revoked if necessary [9].

2.2 Variations of the Authorization and Authentication Procedure

The approaches described so far are either user-dependent, not yet available (validation of sender information) or merely supporting measures (Fraud Detection, Spam Trap and Domain Watch). For reasons like carelessness and ignorance of the users a solution to the problem cannot solely rely on user behaviour. Furthermore a solution should be available soon. The supporting measures alone cannot prevent Phishing, they are just a possibility to quickly react on attacks. Thus the only way to effectively solve the problem is to use methods that change the existing PIN/TAN procedure for authentication and authorization. Therefore we focus on that kind of approach for the remainder of the paper.

Hardware Tokens. The PIN/TAN-procedure is replaced by a small piece of hardware (hardware token) that is given to all users and that can be used to generate one-time-passwords.

- According to [12] AOL uses RSA Security's SecurID hardware token. In order to log in, users have to type in a 6-digit-Code displayed by the token and changed every minute, in addition to their regular password.
- A one-time-password token provided by Kobil Systems does not change the passwords periodically but on user request. Every time the user needs a password he has to push a button on the token [13].
- A third method is used by the Swedish SEB-bank. It uses a token-based challenge-response-system [14]. When logging into the bank website with his ID the user activates his hardware token by entering a PIN. He is shown a challenge that he has to enter in his token. The response (that is only valid for 30 seconds) is then computed by the token and has to be transmitted to the website by the user.

PKI and Digital Signature. When using a Public-Key-Infrastructure (PKI) the user usually gets a key pair and a certificate guaranteeing the authenticity of his public key. A time stamp and a digital signature is then added to every

request sent to the service provider. The service provider can subsequently verify the request by using the users public key. Thus this approach can guarantee authenticity and integrity of the transmitted data if the private keys are kept absolutely confidential and the mapping between a party and its public key is correct. Usually the private key is stored on a smartcard that is protected from unauthorized access by a PIN. For the effectiveness of the time-stamp the clocks of the participating parties should be synchronized.

3 New Proposal

The mechanisms against Phishing shown in the previous sections either need proper behaviour of the user or additional soft- or hardware. But equipping all users with additional soft- and/or hardware can be very costly and there are additional costs associated with installation and user support. Therefore we propose a new procedure that avoids additional hardware.

3.1 How it Works

The new proposal is mainly the combination of the known PIN/TAN-approach with a paper-based challenge-response-technique. It differs from PIN/TAN in the way that the user gets a list with challenge-response-pairs instead of a list with TANs. Before completing a transaction a challenge is presented to the user who must enter the corresponding response. If the response is incorrect the transaction is not carried out.

If the new technique should (also) be used for access control the user has to enter his ID and then sees a challenge from his list (see Fig. 3). If he enters the correct response he is granted access. If he finally wants to carry out a transaction he has to complete the challenge-response procedure again.

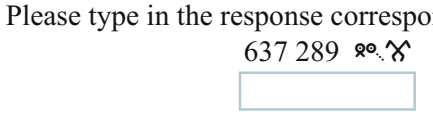

Fig. 3. Challenge-Response Input-Screen

Any challenge is sent to the user only once regardless of the fact if the response was correct or not. If nearly all challenges of the list are used the user gets a new list. After a predefined number of failed attempts to enter the correct response (e.g. three) the user should be notified and his account should be locked (at least temporary). To complicate man-in-the-middle attacks it is reasonable to limit the validity of the challenge to a short period of time so that the attacker only has little time available to act.

The usability is increased if challenge and response are clearly distinguishable. This could be achieved by using a sequence of numbers as challenge and a

Never give a challenge away!

Challenge	Response
037 490	ZSJUFS
193 887	HAGTUH
~~283 749~~	~~BSUNBI~~
~~345 938~~	~~XNAJSK~~
473 648	OKALSZ
637 289	WQNNIV
~~836 445~~	~~IHEUCNP~~
837 465	AFSOPN
...	...

Fig. 4. Challenge-Response-List

sequence of letters as response. Additionally such a challenge is very easy to find in an ordered list. To prevent attacks that ask the user to give away a challenge with the corresponding response the challenge should include some symbols that simply can't be keyed in (see Fig. 4, symbols taken from the Ewok language). If challenge and response are constructed like shown in Fig. 4 the probability for an attacker to guess the corresponding response to a given challenge is approximately 1 to 308 millions. Crossing out used pairs is not necessary but it can be done to keep the look and feel of the traditional TAN lists.

[15] states that it is a major problem that TAN-lists can easily be copied without the kowledge of the user. He solves this problem by adding a physical layer that has to be scratched away before the user can see the TAN. This approach has two drawbacks:

1. The user always has to carry along the list to be able to conduct a transaction what may result in destroying the physical layer accidentially.
2. In some cases the user may actually want to copy the list, e.g. if he has two residences and doesn't want to sway the list between these.

We propose to employ visual cryptography to solve this problem. The user then gets a sheet of paper and a transparency that he has to keep on two different places. When carrying out a transaction he has to combine these two things to be able to see the challenge-response-pairs. Thus on the one hand the legitimate user can still copy the two things easily, but on the other hand for an adversary it is much more difficult to get the two duplicates unnoticed than just copying one list. In short: employing visual cryptography doesn't protect against copying the list but complicates this process for an attacker.

3.2 Evaluation

The new proposal is evaluated according to the criteria in [16]. Thus it's easily possible to compare it with the PIN/TAN-alternatives evaluated there. [16]

uses a long list of criteria that is limited to the one's relevant for Phishing in this paper. These are the main criterions security, user acceptance and costs. Additionally this paper introduces the criterion "Protection against Phishing". The token based approaches have also been included in the evaluation. Table 1 summarizes the results. Following [16] ++ stands for very good, + for good, ∼ for average, − for substandard and −− for not good.

The currently used passwords and TANs provide no protection against Phishing at all. In contrast using PKI and digital signatures has the potential to protect against Phishing completely because the digitally signed (order-)data cannot be modified unnoticed provided that the user really signs his data (e.g. by using an external tamper-proof signing hardware with data visualisation).

As for hardware tokens there are slight differences in the protection against Phishing depending on the option used: If the one-time-password is changed periodically the scammer has to carry out a man-in-the-middle attack to be able to (mis-)use a grifted password. If the token computes a time independent password on demand of the user he can usually use the password(s) till the victim logs on to the real website again.

The new proposal protects better against Phishing than a method based on the latter type of tokens because the scammer needs the correct response to a specific challenge. And since any challenge is sent to the user only once the scammer cannot get a pool of challenges to trick the user. It is only possible to implement a man-in-the-middle attack. Thus the new proposal proctects against Phishing in nearly the same manner as tokens that generate one-time-passwords periodically.

Paper based lists like the ones used in the new proposal are very reliable but they could be misplaced, stolen or copied. By employing visual cryptography unnoticed copying can be made very difficult. Hardware tokens may – besides of being stolen or misplaced – stop working because of power breakdown or external forces.

There is no installation effort for the user neither with hardware tokens nor with paper based challenge-response-lists. Both alternatives are easy to use but the new proposal seems more applicable than the use of hardware tokens because it works more like the well known PIN/TAN-authentication.

Regarding the criterion wide user spectrum the approaches are similar to passwords. For any new service the user needs a new token or a new list and any method can be used for other applications like authentication at an ATM. The transparency of the methods is very high because the user always knows what he has to do and why. He can completely control what he wants to enter.

The software costs for the two alternatives are low. The new proposal just requires an extension of the PIN/TAN-authentication module that can easily be implemented in most cases. If tokens are used a new authentication module must be implemented or integrated into the system.

There are no additional hardware costs for the new proposal. Just the lists have to be printed but this is similar to the PIN/TAN-method. Due to the similarity to the well known PIN/TAN-approach the training costs are low. The

Table 1. Evaluation of PIN/TAN alternatives from [16], own evaluations *in italic*

	Security		User Acceptance				Costs			
Mechanism	*Protection against Phishing*	Reliability	Installation Effort	Applicability	Wide User Spectrum	Transparency of Method	Software Costs	Hardware Costs	Training Costs	Administration Costs
Password	−−	∼	+	+	+	+	+	+	+	−
New proposal	+	++	++	++	+	++	+	+	+	+
Token: Password periodical	+	+	++	+	+	++	+	−	∼	+
Token: Password on demand	∼	+	++	+	+	++	+	−	∼	+
PKI with smart card support	++	+	+	++	++	++	−	−	∼	∼

administration costs are likely to be lower than for traditional passwords because the users can't forget their passwords any more.

In contrast the token based methods are quite expensive because every user has to get his own token. Also the costs for training and administration are higher than for password based methods because the users have to be taught how to use the tokens.

4 Summary

Reliable protection against Phishing can not be achieved with the existing password and PIN/TAN-mechanism. Thus this method has to be changed to some degree. Using digital signatures is the best solution in terms of security. Unfortunately there are a lot of additional costs for necessary hardware, user training, support, PKI, and so on. Another drawback is that the user is no longer highly mobile because most solutions require a card reader plugged into the PC and the necessary drivers. But in many cases plugging hardware into a PC and installing drivers is nearly impossible e.g. on a journey in an Internet Cafe.

Using hardware tokens with periodically changing one-time-passwords is also a reliable protection against Phishing. But this alternative causes a lot of additional costs for hardware, user training, and support, too. These are lower than the costs associated with using digital signatures but not neglectable. In addition the users won't be willing to take a unique hardware token with them for every service they use.

The new paper-based challenge-response-approach suggested in this paper seems to be a good compromise between security and costs because it protects

nearly as reliable against Phishing as hardware tokens while causing considerably lower costs. The major drawback is that it doesn't protect against man-in-the-middle attacks but this is also true for the alternatives that employ the mentioned hardware tokens. Due to the similarity to the well known PIN/TAN-authentication the additional costs for user training and support are very low. The user's mobility is nearly the same as before, he just needs a single sheet (and probably a transparency) with the challenge-response-pairs for every service he wants to use.

The paper shows that there are many reasonable mechanisms to protect against Phishing. They just have to be implemented by financial institutions, web retailers and other service providers.

References

1. FBI National Press Office: FBI Says Web "Spoofing" Scams are a Growing Problem, Washington D.C. (2003) http://www.fbi.gov/pressrel/pressrel03/ spoofing072103.htm.
2. Anti-Phishing Working Group: Proposed Solutions to Address the Threat of Email Spoofing Scams. (2003)
3. Anti-Phishing Working Group: Phishing Activity Trends Report. (2005) http://www.antiphishing.org/APWG_Phishing_Activity_Report-January2005.pdf.
4. Litan, A.: Phishing Victims Likely Will Suffer Identity Theft Fraud. (2004)
5. Nassauische Sparkasse: Tipps zur Sicherheit gegen Phishing-Attacken. (2004) http://www.naspa .de/05_ebanking/05_6_7_tipps_phishing.php.
6. heise news: Phishing-Tricks werden immer ausgefeilter. (2004) http://www.heise.de/newsticker/meldung/52935.
7. Bundesverband deutscher Banken: Online-Banking-Sicherheit. Informationen für Online-Banking-Nutzer, Berlin. (2004) http://www.bdb.de/index.asp?channel=901010.
8. Chou, N., Ledesma, R., Teraguchi, Y., Boneh, D., Mitchell, J.C.: Client-side defense against web-based identity theft. (2004) http://crypto.stanford.edu/SpoofGuard/webspoof.pdf.
9. Dragoon, A.: Fighting Phish, Fakes and Frauds. (2004) http://www.cio.com/archive/090104/phish.html.
10. Böhm, H.: Phishing-Betrüger bevorzugen den Finanzsektor, Wien. (2004) http://www.zt-prentner.at/phishing/Pressemitteilung%20Phishing%20Long.pdf.
11. heise news: Anti-Spam-Arbeitsgruppe MARID der IETF streicht die Segel. (2004) http://www.heise.de/newsticker/meldung/51379.
12. Financial Times Deutschland: AOL bringt neues Sicherheitskonzept gegen Phishing-Mails. (2004) http://www.ftd.de/tm/me/1095597904304.html?nv=wn.
13. KOBIL Systems GmbH: Whitepaper KOBIL SecOVID. (2003) http://www.kobil.de/d/support/download/documents/Whitepaper_SecOVID_ver31_20030519.pdf.
14. Schmidt, N.: Tokens statt PIN/TAN: Sicheres Online-Banking ohne Kartenleser. (2004) http://www.zdnet.de/itmanager/tech/0,39023442,39125970,00.htm.
15. Oppliger, R.: Sichere streichlisten. digma. Zeitschrift für Datenrecht und Informationssicherheit **1** (2005) 34–35
16. Essmayr, W., Leonhardsberger, H., Probst, S., Stockner, W., Weippl, E.: Qualitative evaluation of authentication approaches for ebanking. Technical Report SCCH-TR-0215, Software Competence Center Hagenberg, Hagenberg (2001)