Phishing Attacks and Solutions

Mohamad Badra
CNRS, LIMOS, UMR 6158
Campus des Cézeaux, 63173 Aubière cedex, France
+33 4 73 40 73 58
badra@isima.fr

Samer El-Sawda, Ibrahim Hajjeh
ESRGroups
82 rue Baudricourt
75013 Paris, France
{ibrahim.hajjeh,samer.el-sawda}@esrgroups.org

ABSTRACT

Phishing is a form of online identity theft employing both social engineering and technical subterfuge to steal user credentials such as usernames and passwords. Targeted data sources include especially Web pages, email spam, domain names. Mounting a phishing attacks may take several ways but the popular one takes the form of a phishing message arrives in the user mailbox pretending to be from a bank, directing the user to a web page and asking him to enter his credentials, but the web page is not one actually associated with the bank. In this paper, we focus on the Web site phishing, in which available solutions are based either on providing early warning of suspicious activity and rapid response or on the use of TLS (Transport Layer Security). We present the TLS-SRP (Secure Remote Password) and TLS-PSK (Pre Shared Key) protocols and we demonstrate how these two solutions can be useful to reduce the Web site phishing threats.

Keywords

TLS, Public Key Infrastructures, Phishing, SRP, RSA, Diffie-Hellman.

1. INTRODUCTION

Nowadays, Internet is playing an increasingly significant role in on-line commerce and business activities. However, poor security on the Internet technology and the large financial gains provide a strong motivation for attackers. Internet security risks have increased exponentially as on-line services have become more popular. The risks represent any malicious and undesirable event on the various applications, which possibly suffer from faults facilitating treat concretization. Risks can result in sniffing and hijacking sensitive and personal data over the link for unprotected Internet access. In this paper, we focus on web site phishing.

Web site phishing attacks usually start with an e-mail that arrives in the user mailbox pretending to be from what appears to be a legitimate and known entity. Usually, the mail claims some urgent steps to be taken by the user and direct him to a web page asking him to enter private information like his password. But the web page is not one actually associated with the bank. Gartner Group pointed out that 57 million US consumers have received a phishing e-mail in 2006. Almost 2 million checking accounts have been attacked, leading to an estimated $2.4 billion in fraud [12]. According to the APWG (Anti Phishing Working Group), more than 316736 different phishing attacks were reported between April 2006 and 2007 [11]. In April 2007, the number of unique phishing websites detected by APWG rose to 55 643.

A common factor among all phishing sites is that they maliciously mislead users to believe that they are other legitimate sites. Therefore, detecting phishing pages is essentially an authentication problem between users and servers. Web applications usually involve the user's authentication before getting access to the requested resource. User authentication levels vary from simple to strong; depending on the security politics become applying on the service or resource. For example, a clear-text password-based authentication will be sufficient to enter a Web forum whereas an online banking requires the use of certificates and of public key infrastructures. Nowadays, TLS (Transport Layer Security) [1] is the de facto standard for securing Web and e-commerce transactions. Its native integration in browsers and Web servers makes it the most frequently deployed security protocol. Unfortunately, TLS itself cannot resist entirely against spoofing and phishing attacks (see section 3) and usually relies on browsers to check and validate the entity certificate. Consequently, several solutions have been proposed at the application layer by the browsers vendors in order to protect their users from phishing. These solutions, however, require modifications at the application layer and create interoperability and scalability problems. In this paper, we examine the case of users authenticating web sites in the context of phishing attacks and we analyze and recommend some solutions that can be implemented at the transport layer.

This paper is constructed as follows. Section 2 briefly introduces some phishing attacks and solutions. In section 3 we describe TLS, its integration in web browsers and its weaknesses against Web site phishing. In this section, we present two solutions that can minimize the Web site phishing threat. Finally, we give some concluding remarks.

2. II. PHISHING ATTACKS, SOLUTIONS AND REQUIREMENTS

The phishing problem has evolved significantly over the past few years. This problem touches multiple points across the organization from end users and Web sites to mail servers and networks [15]. In addition, today's attacks come from multiple vectors:

MOBIMEDIA 2007, August 27-29, Nafpaktos, Greece
Copyright © 2007 ICST 978-963-06-2670-5
DOI 10.4108/ICST.MOBIMEDIA2007.1899

- deceptive attacks (spear phishing), in which users are tricked by fraudulent messages into giving out information,
- domain-based attacks (pharming style), in which the lookup of host names is altered to send users to a fraudulent server,
- malicious code-based or Trojan-based attacks, in which malicious software causes data compromises.

Given both the current sophistication and rapid evolution of phishing attacks, a comprehensive catalogue of technologies employed by phishers is not feasible. Some phishing attacks are discussed below.

2.1 Phishing attacks

2.1.1 Rock Phishing Kit

In this method, the phishing email points to a proxy [TCP port re-director] that gets its content from a central spoofed website. Since multiple proxies are used essentially tapping a botnet, it is very difficult to shut down the attack until the central spoofed site is located and the attack can be decapitated [13].

2.1.2 Keyloggers

Keyloggers are spyware programs that install themselves either into a web browser or as a device driver. They are designed to record user input events and activities by monitors keyboard and mouse input and send them to a phishing server (spyware owner). If a keylogger gets into a corporate network, the data leaks could be catastrophic.

2.1.3 Torpig-family Trojan

Torpig-family Trojan, rapidly spreading, is a particularly damaging and technologically advanced session hijacking Trojan. The Trojan monitors major banks' websites worldwide and, after the user logs in, displays a spoofed page while maintaining the original TLS session, thus being very difficult to detect. The Trojan spreads through operating system vulnerabilities [14].

2.1.4 Session Hijackers

Session hijacking refers to an attack in which user activities are monitored, typically by a malicious browser component. When the user logs into its account, or initiates a transaction, the malicious software "hijacks" the session to perform malicious actions once the user has legitimately established its credentials [13]. Session hijacking can be performed locally on a user's computer by malware, or remotely as part of a man-in-the-middle attack.

2.1.5 Content-Injection Phishing

Content-injection phishing refers to inserting malicious content into a legitimate site. The malicious content can redirect to other sites, install malware on a user computer, or insert a frame of content that will redirect data to a phishing server [13].

2.1.6 "Universal" Man-in-the-middle phishing kit

This method can be configured by target, with a very little effort required from the attacker. The MITM kit consists of a PHP file which is installed on a compromised server. The server acts as a proxy between the victims of the phishing attack and the genuine website of the bank. Victims of such an attack receive a regular phishing email. Once they click on the link within the email, they are directed to the compromised server (the proxy) which runs the phishing site. The compromised server communicates with the genuine bank site on behalf of the victim. [14].

2.1.7 Search Engine Phishing

Another approach taken by phishers is to create web pages for fake products, get the pages indexed by search engines, and wait for users to enter their confidential information as part of an order, sign-up, or balance transfer. Such pages typically offer products at a price slightly too good to be true [13].

2.1.8 Spear Phishing

This method is one that focuses on a single user or a department within an organization. The phish appears to be legitimately addressed from someone within that company, in a position of trust, and request information such as usernames and passwords. Spear phishing scams will often appear to be from a well-known entity and may ask employees to update their username and passwords. Once hackers get this data they can gain entry into secured networks [17].

2.2 Phishing solutions

The fight against phishing starts with education and prevention. Users of online services need to learn about what phishing is, the tactics employed by phishers, and how they can protect themselves against attacks [16].

It may be possible to stop a phishing attack at multiple stages. Some countermeasures of phishing attacks, both commercially available and proposed, are discussed below.

2.2.1 Phishing blacklist

Browsers should contact a remote server which holds a phishing domain blacklist. The browser should update the blacklist regularly (phishing sites usually have a lifetime measured in days), and it must report each URL accessed to a malicious remote server.

2.2.2 Bookmarks or history

In this method Bookmarks and history are used to check whether the user had previously visited a site or not. A site can be fraudulent if the user has never visited it before. The disadvantage of this method is that the current history doesn't usually store history for long time.

2.2.3 Two-Way Authentication

When the user registers with online services, it securely receives a unique image, which will be presented to the user in subsequent web site transactions. If a user enters personal identification number at a web site and is presented with the correct secret image, it knows it is dealing with the legitimate institution and can continue to enter its password [14]. But to authenticate itself to the user, the server must display its shared secret that will be captured and then replayed until the user realizes and changes it.

2.2.4 VeriSign Identity Protection (VIP)

VIP is a comprehensive suite of identity protection and authentication services that are designed to strengthen and protect consumers' digital identities. VIP provides invisible server-side monitoring capabilities. It supports thousands of rules and allows organizations to use combination of transaction or user information [15].

2.2.5 Early alarm

This solution is used by some online anti-phishing tools. It consists to define certain rules and checks the security of a Web site according to these rules. This solution provides a toolbar in the browsers to notify its users whether the Web site is verified and trusted.

2.3 Requirements

Phishing is a complex phenomenon in which no one single solution will be able to prevent all phishing. However, reducing the phishing threat can be done if a given solution could meet the following functions: monitoring potentially malicious activity, authenticating email messages, detecting unauthorized use of trademarks or logos or other proprietary imagery, improving the security patching infrastructure to increase resistance to malware, using personalized information to authenticate an email directly to a user and detecting a fraudulent web site and alerting the user.

The given solution should be also able to ensure mutual authentication and to establish a trusted path between the user and a web site. It should also to ensure two-factor authentication, to force passwords to be site-specific and to encode credentials with restrictions on their validity as well.

We briefly discussed some solutions proposed at the application layer. These solutions require modifications to the browsers and unfortunately, we don't know enough about their functionalities and their code sources. A better solution should basically based, in our point of view, on TLS and be able to resolve most of the web site phishing but at the transport layer, by extending TLS with extra backward-compatible authentication methods.

3. TLS AND PHISHING

TLS [1] is becoming the de facto standard for securing web transactions. It is natively integrated in all Web navigators and hence an advanced solution to prohibit phishing attacks must be based on that protocol.

TLS is a transaction security standard that provides end-to-end secure communications between two entities with authentication and data protection. It consists of several sub-protocols, specially the Handshake protocol. The Handshake protocol is used to allow peers to agree upon security parameters, authenticate themselves, instantiate negotiated security parameters, and report error conditions to each other. This protocol is used to negotiate the security attributes of a session. Once a transport connection is authenticated and a secret shared key is established with the TLS Handshake protocol, data exchanged by application protocols can be protected with cryptographic methods using the keying material derived from the shared secret.

TLS supports three authentication modes: authentication of both parties, only server-side authentication, and anonymous key exchange. The anonymous mode is strongly discouraged because it cannot prevent man-in-the-middle attacks. With the other two modes, the client and the server rely on the use of certificates and public key infrastructures in order to establish a mutual authentication and to share a secret key. This authentication method requires the use of trusted third parties which are entities facilitating interactions between two end-communicating entities who both trust the third party. The trusted third party, called also the Certificate Authority is able to generate certificates; binding the public key of an entity to its identity. Thus, when an entity receives a certificate, it will or not trust the communicating entity, depending on the validity of the CA signature on the whole certificate. However, some problems related to the Certificate Authorities can happen [8]; especially when a CA may deliver certificates to phisher web server. In any way, it is often not a good solution to rely completely on the CA itself. In 2001, Verisign Inc. issued two Class 3 code-signing digital certificates to an individual who fraudulently claimed to be a Microsoft employee [9].

Even if the communicating parties rely on CAs to establish mutual authentication, the receiver (client) must carefully examine the certificate presented by the sender (server) to determine if it meets their expectations. Particularly, the client must check its understanding of the server hostname against the server identity as presented in the server certificate, in order to prevent man-in-the-middle attacks. However, the server can host multiple virtual servers at a single underlying network address and hence the above checking will not help the client enough. The client and the server can use the "Server Name Indication" extension specified in [10]. However, no one available browser implements such an extension. In the context of web application, some browsers can check the server hostname against the server identity or can verify if the server certificate is self-signed and therefore alert the user through a pop-up. But the questions become: how many people pay attention to browser warnings alerting them to problems with a website certificate? What is the level of the anti-phishing education to urge the user to look for the TLS or SSL "golden lock" as an indicator of a site's legitimacy?

Whatever the user authentication method in use, the problem of checking the legitimacy of the web site will be there. However, others available TLS authentication methods can be used, avoiding the certificate and host name problems. In fact, not all the users can have certificate and it is in practice the rarely case that the user use a certificate to access a web site. The alternative solution is to authenticate the user using pre shared keys or passwords. TLS authentication based-password can be implemented by firstly establishing a TLS session with only the server authentication and then send the user credentials inside the established TLS tunnel. Due to the certificate and host name problems, this method cannot prohibit the phishing attacks.

A good solution against the web site phishing should be able to ensure the user credential privacy, even if the user has sent such credentials to a falsified web server. In other word, even if the user sends its (protected) credentials to a falsified web server (the attacker), this latter will not be able to retrieve and re-use the credentials on behalf of the user to connect to the legitimate web server.

Two actual solutions can be efficient to resist against the phishing attacks. These two solutions extend the TLS protocol with two new authentication methods. TLS-PSK [2] allows the user and the server to establish a mutual authentication without the use of any certificate and instead, it use a shared key pre-installed on the user and the server machines. The second solution is called TLS-SRP, which uses passwords to establish the mutual authentication.

3.1 SRP

SRP [5, 6] is an authentication method that allows the use of user names and passwords over unencrypted channels without revealing the password to an eavesdropper. SRP also supplies a shared secret at the end of the authentication sequence that can be used to generate encryption keys.

SRP specifications use DH (Diffie-Hellman) key exchange algorithm to agree on a shared secret key. More detail about this mechanism may be found in [6].

Table 1. SRP security parameters

Parameter	Meaning
N	A large safe prime (N = 2q+1, where q is prime) All arithmetic is done modulo N.
g	A generator modulo N
(s, I, P)	(User's salt, Username, Clear text Password)
H()	One-way hash function
u	Random scrambling parameter
a, b	Secret ephemeral values
A, B	Public ephemeral values
x	Private key (derived from p and s)
v	Password verifier

Table 1 provides the list of parameters used by SRP. Within SRP, the server chooses randomly a value for the parameter s, computes the password verifier v using the following formula: $x = H(s, p)$; $v = g^x$. The server stocks in its database the parameters I, s and v.

When the client wishes to connect to the server, the authentication exchange will go as shown in figure 1. The SRP exchanges result in sharing a secret key K between the client and the server. This key is computed as following. Both the client and the server compute $u = H(A, B)$. Next, the client computes K as following: $x = H(s, p)$, $S = (B - g^x)^{(a + ux)}$, $K = H(S)$. The server, however, computes K using the following formulas $S = (Av^u)^b$, $K = H(S)$

Note that $(B - g^x)^{(a + ux)} = (v + g^b + g^x)^{(a + ux)}$

$$= (g^b)^{(a + ux)} = (g^a.g^{ux})^b = (A.v^u)^b$$

To complete authentication, both the client and the server need to prove to each other that their keys match. Consequently, the client computes M = H(H(N) xor H(g), H(I), s, A, B, K) and sends the result to the server, which replies with H(A, M, K).

The most important propriety of SRP is that no useful information about the password P or its associated private key x is revealed during the handshake phase. Therefore, a rogue server will not be able to impersonate the legitimate server since the first does not have the value of v to compute the same K.

3.1.1 TLS-SRP

Using SRP as an authentication method for TLS is now available [7] and under IETF standardization. Actual SRP specification use DH for key exchange. The TLS messages will be used to convey the SRP parameters, as illustrated in figure 2. More details about each TLS-SRP message can be found in [7].

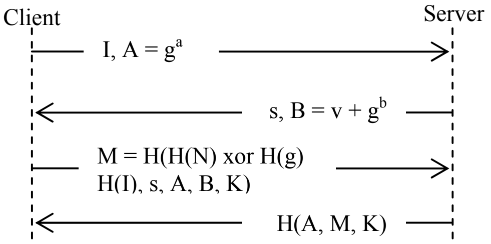
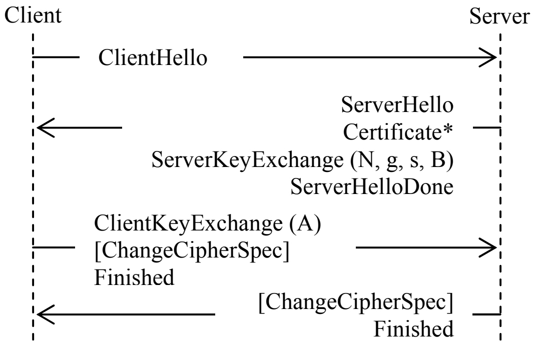


Figure 1. SRP Exchanges.



* Indicates an optional message which is not always sent

Figure 2. TLS-SRP Exchanges.

3.1.2 SRP with RSA

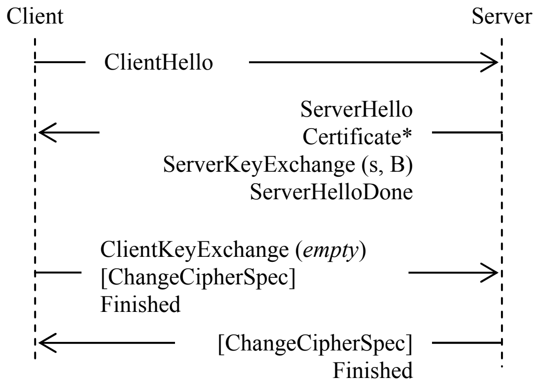
We extend SRP with the use of the RSA key exchange, conserving the SRP soundness. SRP based RSA authentication method uses the following parameters: s, I, p, u, x, and H and defines them in the same way as with SRP based DH (see Table 2). The parameter v is computed as follow: $x = H(s, p)$, $y = H(p, s, I)$, $v = e^{x \| y}$, where || indicates concatenation.

The SRP-RSA negotiation will run as shown in figure 3. The client computes K as following: $x = H(s, p)$, $y = H(p, s, I)$, $S = B^{x \| y}$, $K = H(S)$. The server, however, computes K using the following formulas $S = v^d$, $K = H(S)$. Note that $B^{x \| y} = (e^{x \| y})^d = v^d$.

When using SRP based RSA as an authentication method for TLS, the TLS messages will convey the SRP based RSA parameters in the same way as with SRP based DH. Note that the ClientKeyExchange message will be send empty when SRP based RSA is used. TLS master secret is computed by applying the TLS-PRF function on the K (which replace the TLS pre master secret), the ClientHello.random and ServerHello.random. Thus, the client and the server will be implicitly authenticated via the finished messages. In fact, the finished message is the first protected with generated secrets. Recipients of finished message will verify that the contents are correct and ensure that he is communicating with the legitimate entity.

Table 2. SRP security parameters: RSA case

Parameter	Meaning
N	A large safe integer, N = PQ. P and Q are integer and primes
e	1 < e < PQ, e relatively prime with (P-1)*(Q-1)
v	v has the value $e^{x \| y}$
R1, R2	Random values
B	The server public key, e^d



* Indicates an optional message which is not always

Figure 3. TLS-SRP based RSA Exchanges.

3.2 TLS-PSK

TLS-PSK [2] is another way to establish a mutual authentication using a pre shared key between the client and the server. This method avoids the need for public key operations and the certificates. This protocol was designed to avoid the public key operations and to reduce the TLS overhead when used with performance-constrained environments. However, it can be a good solution to avoid Web site phishing. In fact, TLS-PSK negotiation allows the client and the server to agree upon session keys; applying the TLS-PRF on, among other parameters, the pre shared key. Therefore, without the compromise of the pre shared key, an intruder or a phisher will not be able to compute the same session keys.

This method will not be widely used to avoid phishing attacks since it requires strong keys to be remembered. Thus, users prefer using passwords which are easier to remember, unless they have stocked their credentials on smart cards.

Another method similar to TLS-PSK can also be used, allowing to the server to resume sessions and avoid keeping per-client session state. For more information about this method, please refer to [18].

3.3 General Recommendations

In [4], phishing attacks are classified into five different levels according to their difficulty in detection and prevention. The first 4 levels will be avoided using either TLS-SRP or TLS-PSK. The level 4 is the more difficult to be resolved and in fact it is not related to the security protocol in use, but rather to the system integrity and to the ability of an adversary to install and execute key loggers, Trojans horses or other malicious code.

To avoid the level 4 phishing attack, we suggest using smart cards, which provide trusted and tamper resistant environment and securely store user credentials (shared secrets, RSA private keys, password, etc.). In [3], we presented the first prototype of a TLS smartcard and we demonstrated that today smartcards capacities, in terms of memory sizes and computing power, are sufficient for designing standalone TLS applications.

4. CONCLUSION

In this paper, we analyzed the problem of phishing attacks and the possibility of exploiting vulnerabilities even if strong authentication methods such as TLS based-certificate are deployed. We briefly presented the problem of actual TLS implementations in web browsers and the problem of relying on the Certificate Authority during the certificate verification process. After that, we presented two solutions to countermeasure and to minimize as far as possible the Web site phishing threat. These two solutions are natively integrated at the TLS layer and don't require any modification at the application level and hence, can easily be integrated in all existing web browsers.

5. REFERENCES

[1] Dierks, T., and Allen, C. *The TLS Protocol Version 1.0*. RFC 2246, January 1999.

[2] Eronen, P. (Ed) et. al., *Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)*. RFC 4279, December 2005.

[3] Urien, P., Badra, M., Dandjinou, M. *EAP-TLS Smartcards, from Dream to Reality*. IEEE Workshop Applications and Services in Wireless Networks (ASWN, USA, 2004, 39-45.

[4] Oppliger, R., and Gajek, S. *Effective protection against phishing and web spoofing*. 9th IFIP TC-6 TC-11 Conference on Communications and Multimedia Security (CMS2005), volume 3677 of LNCS, 2005, 32-42.

[5] Wu, T. *The Secure Remote Password Protocol*. ISOC'98, San Diego, CA, 1998, 97-111.

[6] Wu, T. *The SRP Authentication and Key Exchange System*. RFC 2945, September 2000.

[7] Taylor, D., et. al. *Using SRP for TLS Authentication*. IETF Internet Draft (work in progress), December 2006.

[8] Dhamija, R., and Tygar, J. D. *The battle against phishing: Dynamic security skins*. 2005 symposium on Usable privacy and security, New York, NY, USA, July 2005, 77-88.

[9] Microsoft Security Bulletin MS01-017: *Erroneous VeriSign-Issued Digital Certificates Pose Spoofing Hazard*. 2001.

[10] Blake-Wilson, S., et. al. *Transport Layer Security (TLS) Extensions*. RFC 4346, April 2006.

[11] Anti Phishing Working Group. *Phishing Activity Trends Report for the Month of April*. 2007.

[12] Kevin, J., and Delaney, J. *Firms Join Up to Combat Web Fraud*. Wall Street Journal.

[13] Online Identity Theft: *Phishing Technology, Chokepoints and Countermeasures*, available at http://www.antiphishing.org/Phishing-dhs-report.pdf, 2005.

[14] *Phishing special report: what we can expect for 2007?,* www.antiphishing.org/sponsors_technical_papers/rsaPHISH2_WP_0107.pdf, 2007.

[15] *VeriSign Anti-Phishing Solution*. 2006, available at http://www.verisign.com/static/005561.pdf, 2006

[16] *Anti-fraud alliance*. December, 2005; http://www.securitypronews.com/news/securitynews/spn-45-20041117TheAntiFraudAlliance.html.

[17] *All about Phishing*. Mars 2006; http://www.webopedia.com/DidYouKnow/Internet/2005/phishing.

[18] Salowey, J., et. al. *Transport Layer Security (TLS) Session Resumption without Server-Side State*. RFC 4507, May 2007