Journal of the ACS, Vol. 9, May 2018

A Proposal to Protect Against Phishing Attacks

Ahmed ElBagory
College of Computing and Information Technology, Arab Academy for Science, Technology & Maritime Transport, Cairo, Egypt
e.mail:a.elbagory@nilesystem.com

Magdy ElHennawy
Ass. Prof.
High Institute for Computers and Information Systems
Al- Shorouk Academy
Cairo – Egypt
e.mail:mhennawy@ad.gov.eg

Abstract

The diversity of modern networks, the Internet in particular, introduces a lot of facilities. Currently, all commercial applications are tended to be done through the Internet, such as electronic commerce, electronic funds transfer, electronic payment, and so forth. Even the office network environment is now extending to employee's home. The need for authentication and unconditionally secure encryption is essential for today's applications. Every day a new security threats has been discovered. Recently, there is a new security threat, it is the Phishing. Phishing is a robbery operation, but online. It enables the Phisher to get private information such as passwords, usernames, online banking, ATM PIN's and credit card. According to recent figures, the number of Internet users who faced phishing attacks over the last 12 months has grown from 19.9 million to 37.3 million with an increase going over 85 %. Facebook, Yahoo, Google, Amazon and others are among main targets of cybercriminals. The objective of this thesis is to propose a framework to protect against Phishing attacks .The main objective of the proposal is to prevent the Phisher from achieving his attacks.

1 - Introduction

As today's information technology and data networks are used for a broader range of applications, security **[1]** plays an increasingly important role. Before a secure system can be realized, one must first identify the potential security threats. Four basic categories of threats are **[2]**Data disclosure, Fraud, Data insertion, removal, and modification, and Denial of service. Several security services **[3]** have been defined to protect against the threats

identified above, including: Privacy, Authentication, Access Control, Integrity, Non-repudiation, and Replay Prevention.

The primary objective of cryptography is to allow two or more users to communicate securely over an insecure medium, such as the Internet. The same objective is required when somebody tries to enter his sensitive data on a web site such as in e-commerce, banking accounts, or when dealing with cash transfer process. Cryptography can be divided into two categories: symmetric key cryptography **[4][5][6][7]** and public key-cryptography **[8][9] [10].** Together, symmetric key and public key cryptography **[11]** possess the necessary characteristics to achieve information security for a wide variety of systems, including secure electronic commerce and e-mail.

The strength of a cryptosystem can be categorized into two classes: computationally [12] secure and unconditionally secure. A system is said to be computationally secure if the best known attack requires an amount of computational resources which is far too excessive to be a threat in practice. A cryptosystem is unconditionally secured if the cryptosystem is secure against an attack with an infinite amount of resources available. An algorithm, which is based on the difficulty of factoring large composite numbers, is an example of a computationally secure system [5]. An example of an unconditionally secure cipher is the One-time pad (OTP) [4].

Meanwhile, there a set of security threats in which there is a need to other mechanisms besides cryptography. One of such threats is the phishing.

Phishing is the process where a targeted person is contacted by means of email by person who claims to be trusted to get the person's private information such as banking information, credit card information, or passwords. This private information can be, after words, used in an illegal and informal process and can steal assets, information, or even cash from this account **[18]**.

Much of the people who received such malwarecan be told about a big sale or a big offer ona specific website, a famous website, such as (Amazon, Lambert …). The received e-mail contains a link to allow such people to

access the mentioned website. In fact this link is a fake link, leading to a very similar web site to the original one, but a fake one.

Of the above people who clicked on the above mentioned fake link, thevictim, may face one of two cases. In case, clicking on the above mentioned fake link will make the victim to a phishing website.

However, the phisher's hackers have elaborated the phishing process to be a very complicated one in such a way that it is very difficult for normal users to distinguish between the real and infected ones.

In this research we are presenting a proposal to protect against phishing. The paper includes the following sections. It presents the introduction in **section 1**, this section, which introduces an introduction for the need for the information security, the security services, the security protection, the cryptography, as well as the phishing as anew spreading security attack.In **Section 2**, the background about information security and essentiallyof how the phishing attacks work is explained. In **Section 3**, the Fishing related work from other techniques that try to stop this robbery. In **Section 4**, our proposed framework to protect sensitive information against phishing attacks is presented. **Section 5**the feature work and finally, concluding statements are described in **Section 6**.

2 - Background

Information security is the basic issue today's since our daily life becomes a part of the internet and its widely spread applications. Intruders can inflict four major classes of attack on a system: interception, fabrication, modification, and interruption. A fifth class of attacks-repudiation is an attack against the accountability of information. Each of these classes of attacks can be addressed with a security mechanism [13].However, Phising is a crucial threat in today's applications and becomes a real threats against privacy and personal sensitive information. Table 1 summarizes the above attacks, appropriate security services and related protection mechanisms.

Table 1: Attacks, Security Services and Related Protection Mechanisms.

Attack	Security services	Protection Mechanism
Interruption	Confidentiality and Privacy	Encryption/Decryption
Fabrication	Authenticity	Authentication
Modification Replay Reaction	Integrity	Digital Signature for every message
Interruption	Availability	Sort of protection mechanisms, such as DDoS and others.
Repudiation	No repudiation	Digital Signature
Phising	Anti-phishing protection	White and black list

2.1 Interception

Interception is a passive attack on confidentiality where an intruding entity is able to read the information that is sent from the source entity to the destination entity.Example of Interception attack is the eavesdropping and sniffing, gathering information about the network (such as the SSID, the MAC address of the Access Point (AP), and information about whether WEP is enabled) is getting easier with the release of several products [14].

2.2 Fabrication:

Fabrication is an active attack on authentication where an intruder pretends to be the source entity. Spoofed packets and fake e-mails are examples of a fabrication attack.

Examples of fabrication Attack is the man-in-the-middle Attacks. In order to execute a man-in-the-middle attack, two hosts must be convinced that the computer in the middle is the other host [15].Spoofing, is the act of pretending to be someone or something that you are not, such as using another person's user ID and password [14]. Insertion Attacks, the act of configuring a device to gain access to a network or inserting unauthorized

devices into a network in order to gain access is called an insertion attack [14].

2.3 Modification, Replay, and Reaction Attacks

Modification is an active attack on integrity where an intruding entity changes the information that is sent from the source entity to the estimation entity. The insertion of a Trojan horse program or virus is an example of a modification attack. Virus Infection is another issue that affects both wired and wireless networks.

Replay is an active attack on integrity where an intruding party resends information that is sent from the source entity to the destination entity.

Reaction is an active attack where packets are sent by an intruder to the destination. The intruder monitors the reaction [16].

2.4 Interruption

Interruption is an active attack on availability where an intruding entity blocks information sent from the originating entity to the destination entity. Examples are denial of service (DoS) attacks and network flooding. The intruder may try to exhaust all network bandwidth using ARP flooding, ping broadcasts, [15].

2.5 Repudiation

Repudiation is an active attack on no repudiation. Either the source or the destination denies sending or receiving a message.

2.6 Phising

In 1987 the first paper described the phishing technique in International HP Users Group, and in 1990 the term 'phishing' is mentioning in hacking tool AOHell, from this date till now a phishing is one of the biggest forms of electronic fraud**[24] [25]**.

The complete phishing process is done by three parties in coordination. They are the mailers, the collectors, and the cashiers. They are working from different three servers. The aim of working from different servers is to make it difficult to be catch.

The first phisher, the mailer, has the role of sending a millions of fake mails to available normal users. He impersonates a vital entity and send the mails as these mails are received from such entity. **The second phisher**, the collector, have the role to collect the access of the infected users who has access a fake website, for further fake processing. **The third phisher**, the cashiers receives the confidential information from the collector of the infected users, andusesthis information to attack, in a professional way, infected users.

Figure 1 describes the above scenario. In Step 1 the mailer send the fake mail to the user, as an on-line bank entity, ONLINE BANK. In step 2, the infected user sends his confidential information to a fake entity, according to the fake link addressed in the received fake mail, instead of the real one; this is described in step 3, which is directed to the collector. As the collector gives such confidential information to the cashier, as des cribbed in step 4 and step 5, the cashier starts to badly use the confidential information against the infected users.

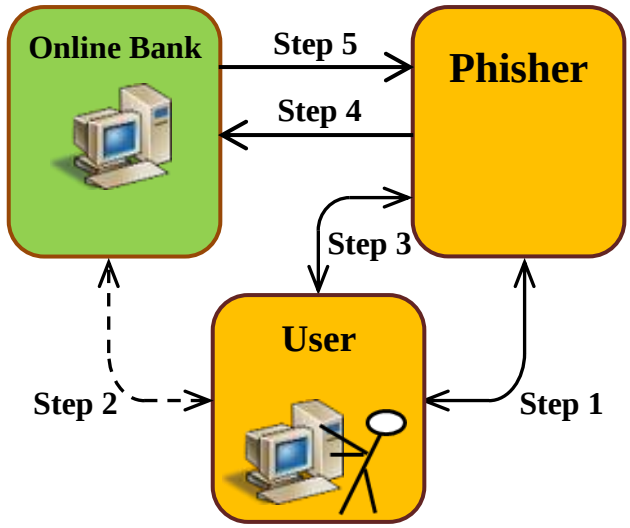

Figure 1: Fishing Scenario

3 –Fishing Related Work

In recent years the number of phishing sites increased, the number of unique phishing reports submitted to APWG during Q3 2017 was 296,208, nearly 23,000 more than the previous quarter**[17][15]**.On the other hand, thenumbers of users that have been exposed to phishing attacks are ingradual increase and the phishing process has become more fatal.

Meanwhile, the protecting techniques that are trying to counter or overcome such attacks are developed. The There are about four basic techniques that have been surveyed yet. They are 'Protecting Users Against Phishing Attacks with AntiPhish', 'An Intelligent Anti-phishing Strategy Model for Phishing Website Detection', 'Anti-Phishing Technique to Detect URL Obfuscation', and 'PhishShield: A Desktop Application to Detect Phishing WebPages through Heuristic Approach' [**20**] [**22**] [**21**] **[23]**.

The above techniques and other techniques are trying to stop this robbery. Since the phishing attacks are growing, so, we are try to reduce its effects through our mentioned proposal.

4 - The Framework of our Proposal

We have implemented this proposal to protect from the Phishing Attacks. This algorithm provides the multilayer security,because of the use of two layers of protection to avoid the possible much number of phishing attacks. As we know, the hackers have elaborated the phishing process to be a very complicated.So,itis complex to detect all that attacks but our algorithm can detect as much as possible the number of this attacks because of it performs the multiple tests such as extensiontest, whitelistand blacklisttest. The whitelist we used is built on the previous results.

Input: Content of Email.
Output: Result of scan (found phishing or not).
Starting with e-mail content, looping on email content, word by word.

The first test is to check the existence of the link or URL in the white list of user account. If so, it means the URL is right and accepted as good URL. If not, we will be obliged to go to the next test. In the next test, we check the existence of the link or URL in black list. If so, it means the URL is fake and not accepted as good URL. If not, we will be obliged to go to the final test.In the this test, we check if extensionis correct, it means the URL is right and accepted as good URL. Else the URL is fake and not accepted as good URL.

Finally, we will be able to add a new URL in the white list if the URL is accepted as good URL.

The idea of the proposed frame work depends on the matching of the received URL with a built-in black list and white list. Besides, it depends on some features like attachment names extensions. It verifies whether they are real extensions or fake ones. **Figure 2,** describe the above proposal.

5 - Future Work

The above proposal is an elementary one, based on the available details. In the future work we assume another tests can be achieved to proof more complete framework with much efficient results.

6 - Conclusion

In this research, we develop proposed framework against the phishing attack. Our Algorithm expects to check and avoid the maximum fake URLs. Our proposal tries to survey the appropriate tests to minimize the fishing attack.

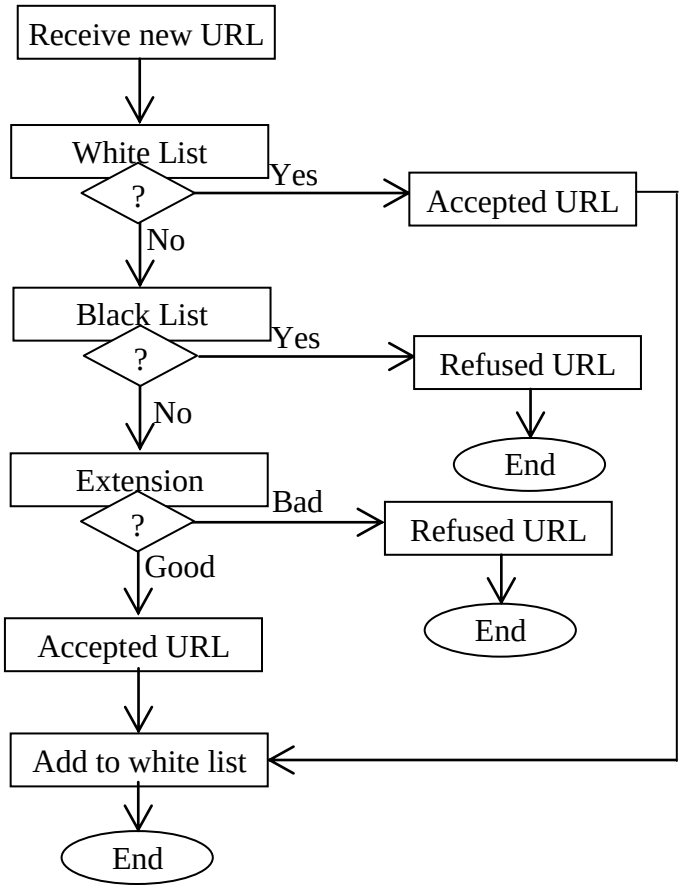

Figure 2: describe the above proposal

References

[1] A. R. S. Ahmed, "Secure Computer Communication and Databases Using Chaotic Encryption Systems", Phd at Electronic Engineering Laboratory, University of Kent, Canterburg, Kent, England, (2000).

[2] Stalling W., Ph.D "Network and Internetwork Security", Printic Hall, (1995).

[3] Carl M. Ellison, Intel Security Technology Lab. "The nature of a usable PKI", Computer Networks, (1999)

[4] Dorothy E., and Denning R., Purdue University, "Cryptography and Data Security", Addison-Wesley Publishing Company, (1983)

[5] BRUCE SCHNEIER, "Applied CryptographyY, Second Edition", John Wiley & Sons, Inc, (1996)

[6] Atkins D., Buis P., Hare C., Kelly R., Nachenberg C., Anthony B. Nelson, Phillips P., Ritchey T., Sheldon T., and Snyder J., "Internet Security, Professional Reference", New Riders Publishing, Indianapolis, IN, (1997)

[7] Daemen J., Govaerts R., and Vandewalle J., " Weak keys for IDEA", In Advances in Cryptology Crypto '93, pages 224-231, Springer-Verlag, (1994)

[8] Brassard G., "Lecture Notes in Computer Science" Modern Cryptology, Edited by G. Goos and J. Hartmanis, (1988)

[9] G. Goos and Hatmanis "Modern Cryptology, A Tutorial, Lecture Notes in Computer Science", Springer-Verlag, (1988)

[10] T. EL GAMMAL, Member IEEE, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms" IEEE Transactions on Information Theory, Vol. IT-31, No 4, July (1985)

[11]Charles P. Pfleeger the University of Tennesseem "Security in Computing" 1989, Prentice-Hall International, Inc.

[12] A. Menezes, P. Van Oorschot, and S. Vanstone, "Handbook of Applied Cryptography", CRC Press, (1997

[13] Frank Ohrtman, and Konrad Roeder, "Wi-Fi Handbook Building 802.11B Wireless Networks," McGraw-Hill 2003.

[14] Randall Nichols, and PanosLekkas, "Wireless Security Models, Threats, and Solutions," McGraw-Hill, 2002.

[15] Hao Yang, Fabio Ricciato, Songwu Lu, and Lixia Zhang, "Securing a Wireless World," IEEE Commun. Mag., vol. 94, no.2, pp 442-454, Feb 2006.
[16] Benjamin M.Lail, "Broadband Network and Device Security," McGraw-Hill 2002.
[17] http://www.antiphishing.org/, 2017.The Antiphishing Working Group. Phishing Activity Trends Report.
[18] http://www.phishing.5org/, 2016 Define Phishing.
[19] http://www.statista.com/, 2016 The Statistic Portal.
[20] Protecting Users against Phishing Attacks with AntiPhish, EnginKirda and Christopher Kruegel Dec 2011.
[21] Anti-Phishing Technique to Detect URL Obfuscation, JigarRathodMay 2014.
[22] Anti-Phishing Strategy Model for Detection of Phishing Website in E-Banking, MohsinFida and A. ArokiarajJovith.
[23] The Phishing Guide, Understanding & Preventing phishing attacks. By: Gunter Ollmann, Director of Security Strategy IBM Internet Security System.
[24] The Phishing Guide, Understanding & Preventing phishing attacks. By: Gunter Ollmann, Director of Security Strategy IBM Internet Security System.
[25] The Ocean Is Full of Phish by Todd Fitzgerald URL: www.nfosectoday.com