Phishing Website Detection and Prevention of Phishing Attacks: a Field Experiment

KARTHIKEYAN R.G, SETHURAMAN R

Lecturer, College of Engineering and Technology, Department of Computer Science and IT, Aksum University.
Lecturer, College of Engineering and Technology, Department of Computer Science and IT, Aksum University.

***Abstract* - The aim of making web users believe that they are communicating with a trusted entity for the purpose of stealing account information, logon credentials, and identity information in general. This attack method, commonly known as "phishing," is most commonly initiated by sending out emails with links to spoofed websites that harvest information. This paper covers the technologies and security flaws Phishers exploit to conduct their attacks, and provides detailed vendor-neutral advice on what organizations can do to prevent future attacks. Security professionals and customers can use this comprehensive analysis to arm themselves against the next phishing scam to reach their in-tray.**

Keywords: Phishing – Prevention of Phishing – Phishing Website detection – Phishing attacks.

I. INTRODUCTION

Phishing is a significant problem involving fraudulent email and web sites that trick unsuspecting users into revealing private information. Phishing has become more and more complicated and sophisticated attack can bypass the filter set by antiphishing techniques. Most phishing emails aim at withdrawing money from financial institutions or getting access to private information and is a serious threat to global security and economy. Phishing filters are necessary and widely used to increase communication security.

Phishing scams have been receiving extensive press coverage because such attacks have been escalating in number and sophistication. Many online service providers believe that their reputation is at stake and fear that users will lose confidence in electronic commerce.

According to a study by Press Trust of India, December 03, 2013, Indian companies lost around USD 53 million (about Rs. 328 crore) due to phishing scams with the country facing over 3,750 attacks in July-September this year, making it the fourth most attacked nation globally, a report by leading IT services firm EMC said. Globally, firms lost USD 1.7 billion on account of cyber criminals launching 1,25,212 phishing attacks in July-September 2013, witnessing a rise in attack volume compared to the second quarter, says Anti-Fraud Command Center's (AFCC) fraud report for Q3 2013, prepared by EMC's security division RSA.

RSA is a provider of security, risk and compliance management solutions for business acceleration. Phishing involves sending emails purporting to be from reputable firms to unsuspecting individuals and also corporate entities to induce then in revealing personal and financial information like passwords, credit card numbers, etc.

RSA ranked India the fourth most targeted country by phishing attacks, receiving 3 percent of the total volume. Other countries targeted by phishing attacks were US (53 percent), Germany (17 percent), the UK (8 percent) and South Africa (3 percent), it said.

India ranks third in phishing attacks on brands with 7 percent of the total volume worldwide. The US with 27 percent tops the chart followed by the UK with 12 percent. AFCC is a 24x7 war-room that detects, tracks, blocks and shuts down phishing, pharming and Trojan attacks perpetrated by online fraudsters.

By understanding the tools and techniques used by professional criminals, and analyzing flaws in their own perimeter security or applications, organizations can prevent many of the most popular and successful phishing attack vectors.

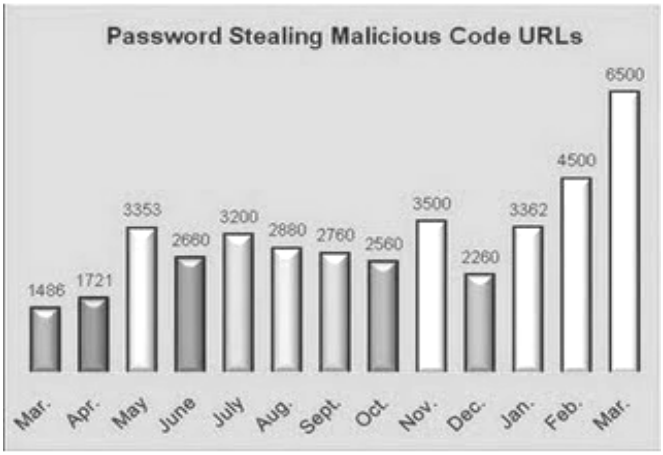
II. THE PHISHING THREAT

Social Engineering Factors

Phishing attacks rely upon a mix of technical deceit and social engineering practices.

The following graph showing number of phishing websites increasing day by day.

In the majority of cases the Phisher must persuade the victim to intentionally perform a series of actions that

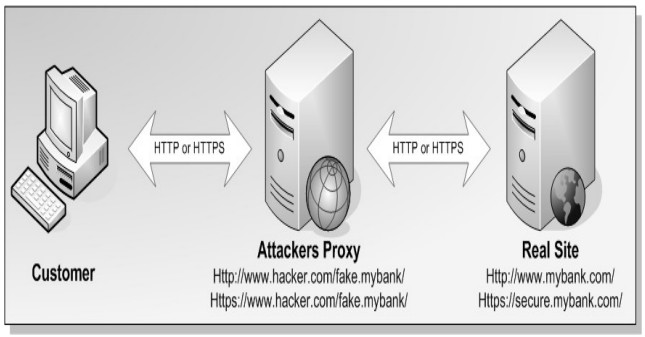


will provide access to confidential Information. Communication channels such as email, web-pages, IRC and instant messaging services are popular.

In all cases the Phisher must impersonate a trusted source (e.g. the helpdesk of their bank, automated support

ISSN: 2278 – 7798

response from their favourite online retailer, etc.) for the victim to believe.



To date, the most successful Phishing attacks have been initiated by email – where the Phisher impersonates the sending authority (e.g. spoofing the source email address and embedding appropriate corporate logos).

III. DEFENCE MECHANISMS

For best protection, these security technologies and techniques must be deployed at three logical layers:

A. The Client-side – this includes the user's PC.

At the client-side, protection against Phishing can be afforded by:

- Desktop protection technologies
  - *Local Anti-Virus protection*
  - *Personal Firewall*
  - *Personal IDS*
  - *Personal Anti-Spam*
  - *Spyware Detection*
- Utilization of appropriate less sophisticated communication settings.
- User application-level monitoring solutions.
- Locking-down browser capabilities;
- Digital signing and validation of email;

To help prevent many Phishing attack vectors, web browser users should:

- Disable all window pop-up functionality
- Disable Java runtime support
- Disable ActiveX support
- Disable all multimedia and auto-play/auto-execute extensions
- Prevent the storage of non-secure cookies
- Ensure that any downloads cannot be automatically run from the browser, and must instead be downloaded into a directory for anti-virus inspection.

B. The Server-side – this includes the businesses Internet visible systems and custom applications.

At the client-side, protection against Phishing can be afforded by:

- *Improving customer awareness*
- *Providing validation information for official communications*
- *Ensuring that the Internet web application is securely developed and doesn't include easily exploitable attack vectors.*

To overcome a Preset Session attack, developers should ensure that their application functions the following way:

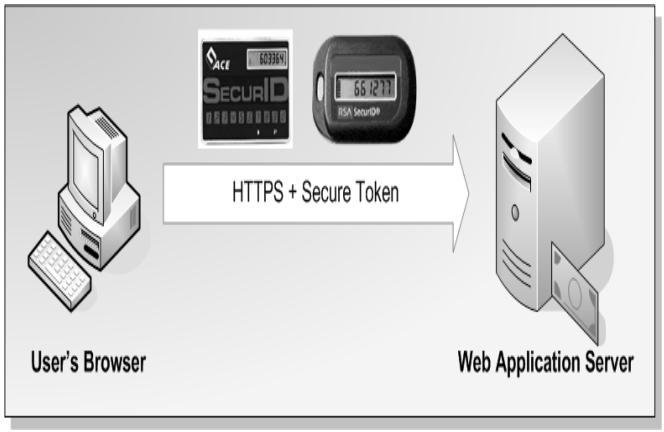
- Never accept session information within a URL.
- Ensure that SessionID's have expiry time limits and that they are checked before use with each client request.
- The application should be capable of revoking active SessionID's and not recycling the same SessionID for an extended period.

- Any attempts to submit an invalid SessionID (i.e. one that has expired, been revoked, extended beyond its absolute life, or never been issued), should result in a server-side redirection to the login page and be issued with a new SessionID.
- Never keep a SessionID that was initially provided over HTTP after the customer has logged in over a secure connection (i.e. HTTPS). After authenticating, the customer should always be issued a new SessionID.

Using strong token-based authentication systems

There are a number of authentication methods that make use of external systems for generating single-use or time-based passwords. These systems, often referred to as token-based authentication systems, may be based on physical devices (such as key-fobs or calculators) or software. Their purpose is to create strong (one-time) passwords that cannot be repeatedly used to gain entry to application.

Customers of the legitimate web-based application may use a physical token such as a smartcard or calculator to provide a single-use or time-dependant password.



C. Enterprise Level – distributed technologies and third-party management services

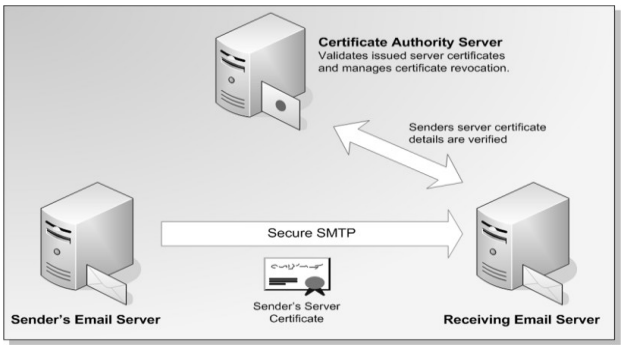
A key step to anti-phishing enterprise-level security includes:

ISSN: 2278 – 7798

- *Automatic validation of sending email server addresses,*
- *Digital signing of email services,*
- *Monitoring of corporate domains and notification of "similar" registrations,*
- *Perimeter or gateway protection agents,*
- *Third-party managed services.*

a) Anti-Phishing Plug-ins

There is a growing number of specialist anti-phishing software producers that provide browser plug-ins. Most often, the plug-ins are added to the browsers toolbar and provide an active monitoring facility. These toolbars typically "phone-home" for each URL and verify that the requested server host is not currently on a list of known Phishing scams.



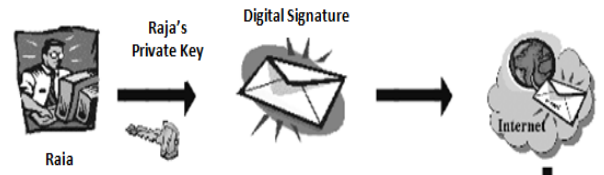
b) Digitally Signed e-mail

It is possible to use Public Key cryptography systems to digitally sign an email. This signing can be used to verify the integrity of the messages content – thereby identifying whether the message content has been altered during transit. A signed message can be attributed to a specific users (or organizational) public key.

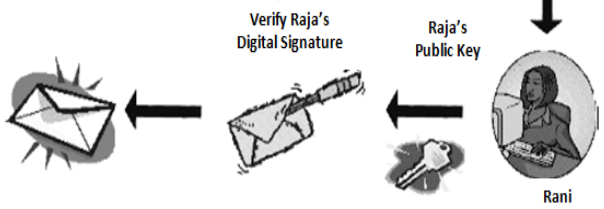
Almost all popular email client applications support the signing and verification of signed email messages. It is recommended that users:

- Create a personal public/private key pair
- Upload their public key to respected key management servers so that other people who may receive emails from the user can verify the messages integrity

1. Raja stamps his digital signature to the email by using his private key and then sends the email to Rani.



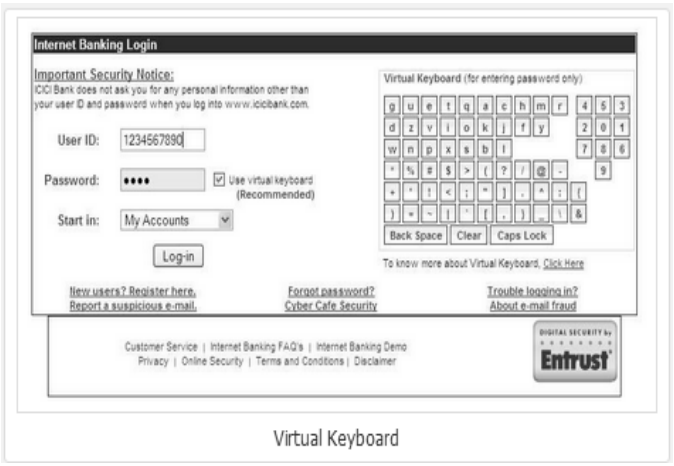
2. Upon receiving the email, Rani verifies the digital signature in the email with Raja's public key



- Enable, be default, the automatic signing of emails
- Verify all signatures on received emails and be careful of unsigned or invalid signed messages – ideally verifying the true source of the email.

Pierluigi Paganini of Infosec Institute advocates prevention is better than curing in this case, and suggests a few guidelines to fight the phenomenon:

- Verify online accounts regularly;
- Never divulge personal information via phone or on insecure websites;
- Don't click on links, download files, or email attachments from unknown senders;
- Beware of pop-ups. Never enter personal information in a pop-up screen.



Virtual Keyboard

- The login window does not have virtual keyboard which is very important shield to fraud cases, when user keystrokes are being recorded. Bank Website provides this. Example, ICICI bank website.
- In any case, the script should be written so that browser cannot store username and / or password even if user forces.

IV. CONCLUSION

- Although phishing scams have received extensive press coverage, phishing attacks are still successful because of many inexperienced and unsophisticated Internet users.
- Attackers are employing a large number of technical spoofing tricks such as URL obfuscation and hidden elements to make a phishing web site look authentic to the victims.
- By understanding the tools and technologies Phishers have in their arsenal, businesses and their customers can take a proactive stance in defending against future attacks. Organizations have within their grasp numerous techniques and processes that may be used to protect the trust and integrity of their customers personal data. The points raised within this paper, and the solutions proposed, represent key steps in securing online services from fraudulent phishing attacks – and also go a long way in protecting against many other popular hacking or criminal attack vectors.
- By applying a multi-tiered approach to their security model (client-side, server-side and enterprise)

ISSN: 2278 – 7798

organizations can easily manage their protection technologies against today's and tomorrow's threats – without relying upon proposed improvements in communication security that are unlikely to be adopted globally for many years to come.

- The most effective solution to phishing is training users not to blindly follow links to web sites where they have to enter sensitive information such as passwords.
- However, expecting that all users will understand the phishing threat and surf accordingly is unrealistic. There will always be users that are tricked into visiting a phishing web site. Therefore, it is important for researchers and industry to provide solutions for the phishing threat.
- One of the most important ways to mitigate cyber attacks and data breaches is to share information about major incidents and cybercrime trends. Banks, law enforcement and intelligence agencies must cooperate to prevent further damage and mitigate cyber threats that are even more sophisticated.

REFERENCES

[1] "Proposed Solutions to Address the Threat of Email Spoofing Scams", the Anti-Phishing Working Group, December 2003.
[2] "http://resources.infosecinstitute.com/phishing-counter-measures-unleashed" by Chintan Gurjar|October 21st, 2013.
[3] "Anti-Phishing: Best Practices for Institutions and Consumers", McAfee, March 2004.
[4] "URL Encoded Attacks", Gunter Ollmann, 2002
[5] "HTML Code Injection and Cross-site scripting", Gunter Ollmann, 2001.
[6] "Web Based Session Management", Gunter Ollmann, 2002.
[7] "Custom HTML Authentication", Gunter Ollmann, 2003.
[8] "Phishing Victims Likely Will Suffer Identity Theft Fraud", Gartner Research Note, A. Litan, 14 May 2004.
[9] http://securityaffairs.co/wordpress/19010/cyber-crime/online-banking-cyber crime.html, 2013.
[10] "Phishing attacks and countermeasures", Ramzan, Zulfikar (2010).
[11] "Study Finds Web Antifraud Measure Ineffective" By brad stone, February 5, 2007.

ISSN: 2278 – 7798