RESEARCH REVIEW JOURNALS
Volume-03
Issue-12
December -2018

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com [UGC Listed Journal]

Hacking in E-Banking

[1]Shashikant & [2]Dr. Suresh Dara

[1]Research Scholar, Dept of Computer Science, Sri Satya Sai University of Technology and Medical Science, Sehore, MP (India)
[2]Department of Computer Science & Engineering, B.V RAJU Institute of technology, Narsapur, Medak, Telangana (India)

ARTICLE DETAILS

Article History
Published Online: 10 December 2018

Keywords
Hacking, Internet Banking, Crimes, Trojans, Frauds.

ABSTRACT

The role of banking is redefined; customers are also becoming more discriminating and demanding. To meet customer expectations, banks will have to offer a broad range of deposit, investment and credit from a mere financial intermediary to service provider of various financial services under one roof acting like a financial supermarket with maximum security. Thus, the customer-oriented demand on internet banking is increasing continuously because e-banking provides various transactional facilities to its users 24X7 but at the same time banks as well as customers are expected to be aware towards various types of hacking techniques. However, it also brings new possibilities for thieves. This is mainly because we have not completely solved the growing problem of computer viruses and Trojans that can act on our computers against our will. In this section, we have discussed about common hacking techniques by classifying these techniques into two categories classical attacks and new attacks; where examples of classical attacks are password guessing, brute-force attack, eaves dropping and shoulder surfing.

1. Introduction

New attacks we have categorized into two categories, off-line credential-stealing attack and on-line credential-stealing attack. Examples of offline credential-stealing attacks are phishing or brand spoofing, spear phishing, vishing, malware, pharming, skimming and credit card frauds etc; whereas in on-line credential-stealing attack examples are spy ware or key loggers or keystroke logging, worms, Trojans or back-door Trojans, in session phishing attacks, hacking tricks toward security on network environments through - instant messaging, distributed deny of service attack of botnet and payment recipient scams. All the banks, which have implemented as core banking systems, offer e-banking and mobile banking facilities. But with these facilities always there is a question of security i. e. protection of personal information from the thieves. Computer damages have been classified as:

1. Computer Frauds; and 2. Computer Crimes

Computer frauds

The latest fraud which is considered as the safest method of crime without making physical injury is the Computer Frauds in Banks. Computer frauds are those involve misuse or defalcations achieved by corrupting with computer data record or program. Computer fraud is the use of computers, the Internet, Internet devices, and Internet services to defraud people or organizations of resources.

Computer crimes

Computer crimes are those committed with a computer that is where a computer acts as a medium. The difference is however academic only. A few of the methods adopted by fraudsters are: Phishing, Skimming spoofing, credit card frauds etc.

In today's digital world, the prevalence of e-commerce opens a door for various cyber crimes that we have never seen before. Viruses can be written from, and spread on virtually any computer platform.

Virus attack

Attacks are getting more and more aggressive against computers and servers all around the internet. Computer viruses are nothing more than computer programs and therefore can do virtually anything the programmer wants on the computers they infect.

The operating systems used on these computers have a tendency to sacrifice the security on behalf of the commodity of the user. Under such circumstances, its very easy for an attacker to implement a man-in-the-middle attack. This way an attacker could end up controlling the money in our bank accounts. Virus can also attack and used for automating maintenance tasks on the computer, can delete all the data on the hard disk, and encrypt it so that the owner has to pay to get the data restored to its original form, and even steal private data such as documents, system passwords and cryptographic keys.

Attack to the PC bank systems

Actual PC banking systems rely mostly on the use of password authentication systems, jointly with strong cryptographic communication systems. The problem is that these methods are not always robust enough for Internet banking applications. Introducing a login and a password on a secure Web page for authentication is equivalent to keeping the door-key under the doormat, as any program executing on our computer like viruses, Trojans and malwares etc. can have access to them.

We could think that a system such as UNIX**,** where only the operating system can access all the memory, limiting each program to its own memory space, is immune to such an attack. This is definitively wrong. A virus could infect the browser program inserting in it code that steals that information from memory. The operating system cannot distinguish "good"

code from “malicious” code, so it will never notice it. Even more, sometimes it is enough to steal the file where the critical information is stored and the password(s) used to secure it. All we need is a virus that waits until the user introduces the password to access the critical information and then send it over the network with the file where the secret keys are stored.

Even more, sometimes the access password is so simple that we can break it using a dictionary attack.

Viruses

Viruses can be written to work under any known operating system and there are also viruses that can be written on macros such as MS Word macros and java script (a web-based language which allows the introduction of code in web pages). Viruses normally can only be executed with the operating system for which it was created. But even though there are operating systems which are more difficult to attack, such as UNIX, not even these systems are completely safe. Even though it is true there are fewer viruses for these systems, it is also true that they exist and with them the possibility to expose critical information to the leaked without our permission.

2. Classic Attacks

Here, we describe common well-known attacks widely used in history and presence.

Password guessing

Password guessing is usually dictionary based attack, where attacker is trying to guess our password. Usually, dictionary of a lot of common passwords is used. When attack remains unsuccessful after applying predefined set of passwords, then is redirected to another user.

Brute-force attacks

Thorough search known as brute-force attack is based on trying a large number (all) of possibilities of password or secret key. In the following figure a model of simple brute force attack on a Norwegian internet bank has been shown.

As it is clear from the following figure, a hacker selects any Social Security Number (SSN) from the list of customers SSN numbers and then attempts to login using any randomly chosen Personal Identification Number until the correct password is acquired or the attack is detected.

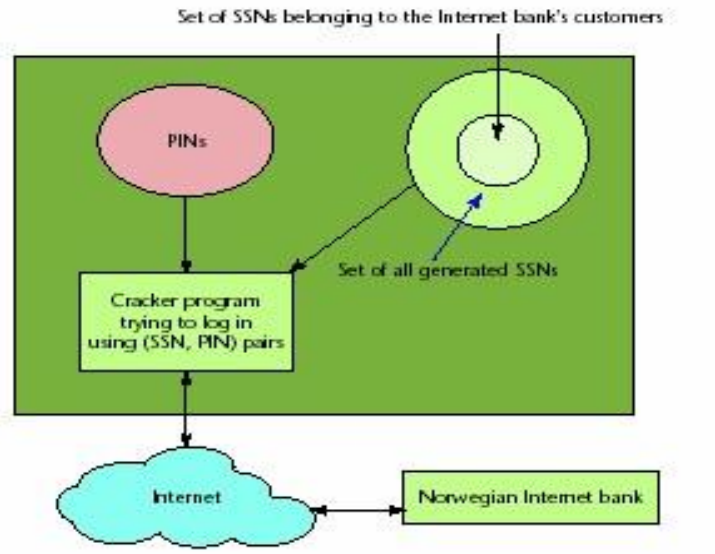

Fig 1: Brute-Force Attack Model

Eavesdropping

Eavesdropping is listening without the speaker’s knowledge. It’s usually used for ManIn-The-Middle (MITM) attack.

Shoulder surfing

One of the oldest and most common threats to our online banking security is "shoulder surfing". This is as simple as having an unauthorized person watching over account holder shoulder as user conduct his online banking session. If this person can view user’s keyboard, they will be able to see the IDs and passwords used to access the system [16]. In this method unauthorized people keeps an eye on that user who is busy in performing their account operations and try to see the IDs and passwords.

3. New Attacks

On the basis of the resistance all internet banking authentication methods can be classified into two common attacks-

- Off-Line Credential-Stealing Attack and
- On-Line Credential-Stealing Attack

Off-line credential-stealing attack

In this type, hackers try to steal user’s private information from those client’s PC’s who have insufficient protection for PC . As it is clear from the following figure that hackers use malicious software’s such as Trojan horse or by tactfully getting user’s identification through phishing and pharming or by combining phishing with pharming.

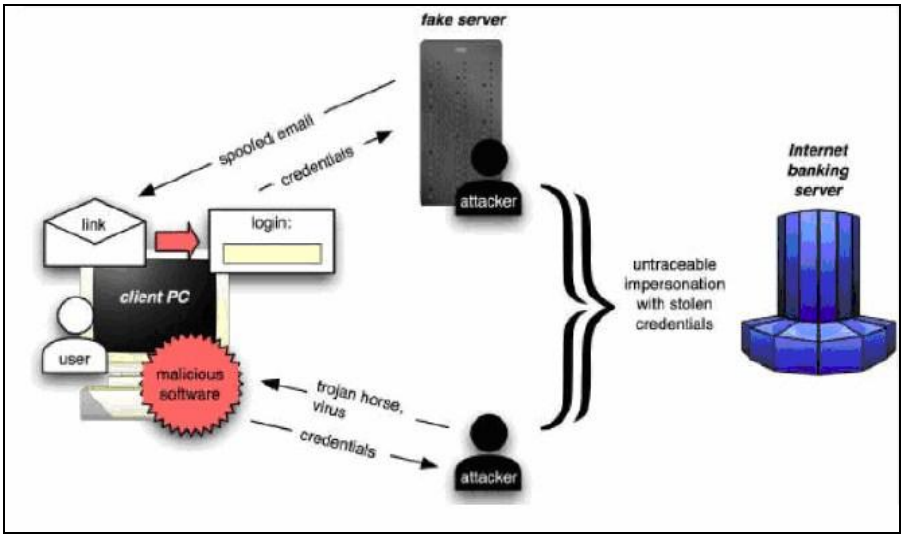

Fig 2: Offline Credential Stealing Attack Scenario

Phishing / carding / brand spoofing

The word "Phishing" first appeared in 1996. It is a variant of 'fishing', and formed by replacing the 'f' in 'fishing' with 'ph.' from phone. It means tricking users of their money through e-mails. It is a form of online identity theft that aims to steal sensitive information from users such as online banking passwords and credit card information from users. The last years have brought a dramatic increase in the number and sophistication of such attacks. 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.

Phishing attacks use a combination of social engineering and technical spoofing techniques to convince users into giving away sensitive information (e.g., using a web form on a spoofed web page) that the attacker can then use to make a financial profit. A method in which hackers capture the trusted brands of well-known financial institutions and tactfully asking users personal identification through false/fake website forms.

These kinds of attacks were harmless so long as user ignored and deleted the e-mail. But if user responded, then they would try their best to get users account information. So, we can define it as *"The act of convincing users to provide personal identification information, such as social security numbers or bank information, for explicit illegal use"*.

Among all the cybercrimes targeting e-banking systems, phishing attack has become one of the most serious threats. In the main form of phishing attack, the criminals (called phishers) setup fake e-banking/e-payment web sites, and then send phishing emails to potential victims, who may be lured to access the phishing sites and expose their sensitive credentials to the phishers. The credentials harvested by the phishers normally include bank account numbers, passwords or PIN numbers, e-banking TAN numbers, credit card numbers and security codes, social security numbers, and so forth. With the collected credentials, the phishers can login the genuine e-banking/e-payment system to steal the victim's money.

There are also many other more advanced forms of phishing attack, such as the following:

- Phishers get phishing sites indexed by some search engines (via some Search Engine optimization tricks) and then wait for victims to visit them;
- Phishers use cross-site-scripting (XSS) to inject links of phishing sites to legitimate sites;
- Spy-phishing (or malware-based phishing): phishers depend on Spyware/ malware like trojan horses and keyloggers to collect sensitive credentials;
- Pharming: phishers misdirect potential victims to phishing sites through DNS poisoning.

Phishers can also tailor the contents of the phishing mails and even those of the phishing sites for targeted victims, which is called spear phishing or context-aware phishing. This kind of phishing attack becomes much easier nowadays, because more and more personal information is publicly available at online social networks. In the following diagram information flow of a typical phishing attack has been shown:

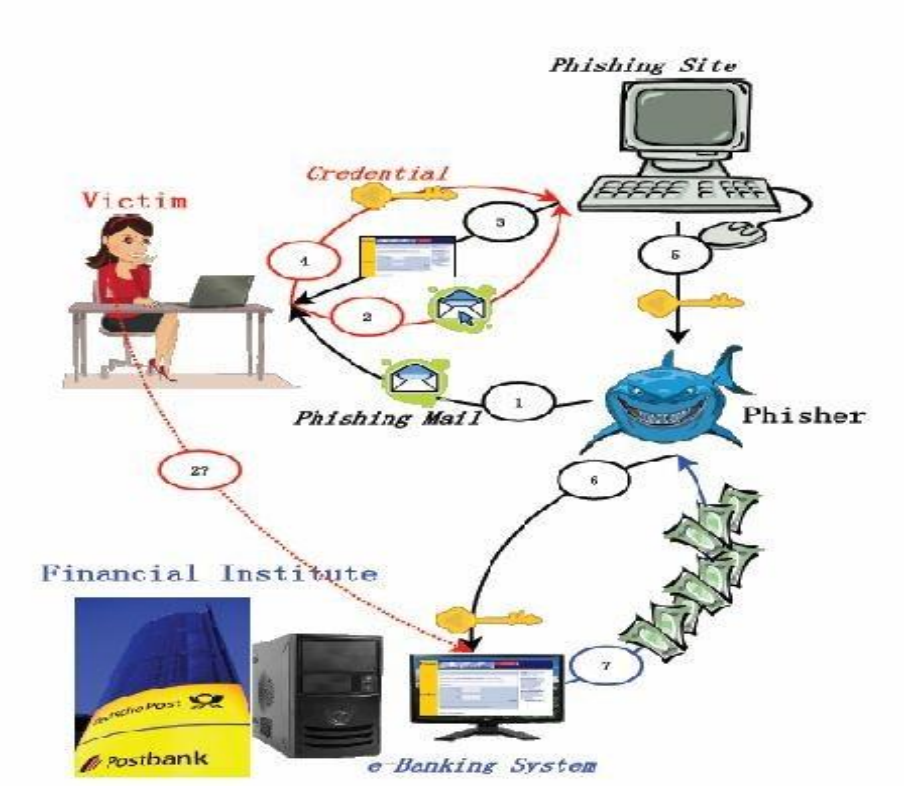

Fig 3: Information Flow of A Typical Phishing Attack

In the above figure we can see seven different steps that can be cut down to stop a phishing attack.

4. Conclusion

Banking and finance sites have the greatest risk for getting hacked. The worst vulnerabilities were found in banking and finance web applications tested by Positive Technologies, a firm that provides internet security products for businesses. Greater complexity results in more opportunities for hackers. The hackers primary target are the average user. "The number-one threat is attacking target web application users. A whopping 87 percent of banking web applications tested by Positive Technologies were susceptible to these attacks. The most common vulnerability was Cross-Site Scripting, which allows attackers to perform phishing attacks, which can result in malware infection. In a phishing attack, the hacker sends, for instance, an email pretending to be a trusted entity like a bank or major shopping site, hoping to dupe into clicking on the malicious link.

References

1. Bogdan Ksi zopolskia, Zbigniew Kotulski (2007), "Adaptable security mechanism for Dynamic environments", computers & security, 2007, pp. 246– 255.
2. Damien Hutchinson, Matthew Warren (2003), "Security for internet banking: a framework", Logistic Information Management, Volume 16, Number 1, 2003, pp. 64-73.
3. Stephen Wison (1999), "Digital signatures and the future of documentation", Information Management & Computer Security 7/2, 1999, pp. 83-87.
4. Ganesh Ramakrishnan (2001), "Risk Management for Internet Banking", Information Systems Control Journal, Volume 6, 2001, www.isaca.org/TemplateRedirect.cfm.
5. Lawrence F. Cunningham, James Gerlach and Michael D. Harper (2005), "Perceived risk and e-banking services: An analysis from the perspective of the consumer", Henry Stewart Publication 1369-0539, Vol. 10, PP. 165-178 Journal of Financial Services Marketing.
6. Gary H. Stern and Ron J Feldman (2006), "Managing Too Big To Fail by Reducing Systemic Risk: Some Recent Developments", Federal Reserve Bank of Minneapolis.
7. Jingdong Cui;(2007), "Consumer Decision Process Model in Multi-channel Retail Banking", International Conference on Service Systems and Service Management, PP: 1 – 6, IEEE Conferences.
8. Jinkook Lee, Jinsook Erin Cho, and Fahzy Abdul-Rahman, (2008), "E-Banking",
9. Department of Consumer Sciences, Ohio State University, 1787 Neil Avenue, Columbus, OH 43210, USA. e-mail: lee.42@osu.edu.
10. Jen-Her Wu, Tzyh-Li Hsia, Michael S H Heng (2006), "Core Capabilities for Exploiting E-banking", Journal of Electronic Commerce Research, VOL 7, NO.2, www.csulb.edu/journals/jecr/issues

