A Theoretical Analysis of Different Hacking Techniques in Wireless Networks

Mr.S.Manimaran
Assistant Professor
Department of Computer Science and Engineering
M.Kumarasamy College of Engineering, Karur, Tamil Nadu, India
E-mail: smaran.1989@gmail.com

S.Kaviya, S.Josphin Anitha, S.Meiyappan
UG Scholars
Department of Information Technology
M.Kumarasamy College of Engineering, Karur, Tamil Nadu, India
E-mail: kaviyasengottiyan@gmail.com, josphinanitha@gmail.com

Abstract— Over the course of past few decades to today's world, even though the usage of computers is increasing rapidly, the users hesitate to store their personal information in their computers because of the security issues of computing. The security issues are embossed because of the hackers. Hackers are also the programmers who unethically make use of our personal information, they may steal it and use for some unwanted purpose. They are greatly motivated by a massive amount of profit, challenge, strong efforts, to assist in performing illegal activities. All hackers do not follow a same technique to perform illegal tasks. It will vary depending upon the security of information and the depth of the content involved in it. There are a large number of hacking techniques available in wireless networks. In this theoretical analysis, the systematic methodology of various techniques that the hacker follows to attack a machine or sensitive information of the users has been scrutinized.

Keywords-Cryptography; Intrusion; Hacking; Spoofing; Encryption; Information Security; Sniffing

I. INTRODUCTION

The term Privacy is highly expected everywhere in the current scenario and is needed by the entire system administrator as well as users. Due to hackers the privacy in every domain is getting declined drastically. Not only stealing the information, they may crash our system too. In order to make whole system secure, there is a thirst for hacking techniques to avoid the information access by hackers. Apart from these, there are also several password attacking issues to be resolved by innovating suitable secure authentication approaches in a specific manner. For doing that the following sections exemplifies the several hacking approaches as well as its recovery mechanisms in order to analyze the working process and its significance.

II. DIVERSE HACKING TECHNIQUES

The following section exemplifies the several hacking approaches as well as its recovery mechanisms in order to analyze the working process and its significance.

A. Heartbleed Bug

This is one major technique used by the hackers based on cryptography. It is considered as a serious flaw in the OpenSSL cryptographic [1] software library. The open software toolkit is an important one which makes the use of secure socket layer and transport layer, provides communication security of networks. This software toolkit is an Openness, which has SSL/TLS for information security in web, e mail etc., By using this technique someone can easily read the system memory protected by OpenSSL. If the hackers attack our systems through OpenSSL [1] they can steal all information without leaving any footprints. By this technique they can easily track the key which was generated during the encryption process. By means of this key they can easily hack our information. There are not memory limitations for this attack.

Here in this technique, there may be a possibility of leakage of the whole memory from server to client or vice versa. Heartbleed is considered as a major issue because we can steal a large amount of information without leaving any evidence. The leaking things are classified into four types, they are as explained below.

1) Primary Key Material: Here the leakage of key is considered as a primary one. If the key is leaked, then all the encrypted information is non-secured. This can be recovered by issuing the new keys. By doing this, we can't ensure that our information is secure. The hacker can hack the information through the past key decryption. This all is done by the person who owned the service.

2) Secondary Key Material: This means the leakage of password and username. After this the user can frequently change their passwords and also encryption technique.

3) Protected Content: The data what the user storing in business suit, application site even the government site can be easily hacked. To avoid this hacking one can implement the primary key security and secondary key security that is mentioned above.

4) Collateral: In addition to the data, there may be a leakage of other information that is the memory address of data and the information about how the user protects the data.

Recovery Mechanism

There is the certain Operating System [1]such as abandoning, centos, fedora, OpenBSD, FreeBSD, NetBSD are affected by this attack. This is not the result of a design defect of OpenSSL. But this is due to the implementation defect. Now the fixedopenSSL has been designed to fix the vulnerability in the previous version of OpenSSL.

B. Man in the Middle Attack

This may happen by using the network communication protocol, which is mainly used for transmission of a message from one system to another. If the client and the server are the two persons who need to communicate are in the same LAN there may be a [2] higher possibility for the existence of man in middle attack. A hacker may present in the middle of sender and receiver and read the entire message between the sender and the receiver [3]. In the server client system the hacker is in the middle of both and collects the request signed by the client and the responses received by the client. The hacker might know the username, password, mobile number, credit card number etc.

In an HTTP transmission both the server and client use the same and single TCP protocol the hacker just break the TCP into two segments. One is between the hacker to the client and another is between the server to a hacker and vice versa. The most important technique used here is ARP Spoofing, the hacker sends the message to the local area network in order to combine his MAC Address [3] to the IP address of sender so that the entire message reaches the hacker instead of the server. The reason for its existence is the usage of unencrypted messages in the network.

Recovery Mechanism

It is very difficult to avoid the ARP Spoofing with the security tools come with the personal computer, so in order to avoid it, the user can use the HTTPS protocol and VPN instead of HTTP. All the HTTPS protocol is working with the SSL (server socket layer) to hide the information from the hackers. Some VPN also makes use of the SSL protocol, if the user wants to use VPN one must have a connection with the VPN access point.

Now while making a connection with a server with HTTPS an identity of a server has been identified that are connected in that stream or security warning will be generated. This assumes that someone is in between. If there is a connection with the VPN access point the same security purpose against Man in Middle Attack can be highly used.

C. POODLE

POODLE (Padding Oracle on Downgraded Legacy Encryption) is one of the hacking techniques where the client and the server use the SSL 3.0. SSL 3.0 is rarely used because it has no security. With practical, SSL 3.0 is replaced by TLS 1.0. TLS is used for providing backward compatibility and interoperability with legacy system. The attacker exploits the downgrade dance to steal the information. POODLE [7] allows us to hack the secure HTTP cookies.

Many TLS clients provide downgraded dance, it helps the hackers to attack. If the client has highest protocol version, but the server does not support the version, at the time the handshake will fail. So the client moved to earlier version protocol, if the server supports the version, then the handshake will be made. The attacker triggers the downgrade. The attacker controls the network connection between client and server with the help of providing handshakes with TLS 1.0.During encryption, SSL 3.0 uses the cipher in CBC mode, the cipher may be blocked or RC4. The cipher is used to leak the message when the same message is sent through different connection. We can attack the CBC encryption with the help of SSL 3.0, and then the user can change the transmission between client and server. SSL 3.0 has no security. The major drawback of CBC encryption with SSL 3.0 is that it has no Message Authentication code, while decryption integrity is not checked.

The disadvantages of SSL 3.0 would be used by the attackers while decrypting. The POODLE attacks were implemented by running the JavaScript to get the sender cookies. After that sender request has been easily modified before reaching the server if the handshake fails again request have to be send. The handshake between server and client is made then the attacker easily steal the information. SSL 3.0 is used in internet explorer. The user who uses the browser would be unsafe, so they use the SSL v3 to support the server, and then they provide a fallback. Apart from that TLS client and TLS server, TLS_FALLBACK_SCSV are used in client and server with different value. Downgraded dance is used for interoperability in TLS client. In TLS server, the connection includes the values such as 0x56,0x00. Originally the information has certain terms like C1… Cn, after the attack the terms are changed in CX.

Recovery Mechanism

Client restricts to use the SSL 3.0 for encryption. Avoiding SSL 3.0 is not possible, for legacy system so SSL 3.0 is highly preferred. Even though using SSL is insecure, but one cannot predict the quality, the only way is that to control the usage of SSL 3.0.

D. Sniffing

Sniffing is one of the hacking techniques, which is more popular in a wireless network. Here, sniffer code is used to see the information between the networks. The sniffer provides the information about the packet that is starting address, ending address and data. Sniffers [6] have certain features that help us to get the data and other information. Certain sniffer has ability to reproduce the files through a network. The most important tool in the hacker's equipment is sniffer. The sniffer gives the information about the data that is IP address and network topology. With the help of the complete information, the user can travel through the network and get the important data that will provide the control to the network. Media Access Control (MAC) address is the network address, sometimes called physical address. The specific network information is accepted by the network card.

There are two types of mode, one is monitor mode and another one is disapproval mode. The monitor mode is exceptional in sniffing. The network card status is used only for the wireless network interface card because the wireless network has individual properties. Even though a card in disapproval mode, it will in wireless networks. The card is not needed to be a part of the network. Here, the sender sends the data is not reached to the network as it sends the data out of the network, then the hacker change the data and again send to the destination address. There are several layers in network communications in that, network layer has higher responsibility. The network layer is used for searching the information for the destination. Every network card has a unique destination address (MAC address). While changing the MAC address, it is mandatory to ensure the connection because if the destination address will not match to the packet address then the packet would be lost. The network card can run in disapproved mode.

Sniffer can be viewed in two types of personality. One type is the person watches and sends replies to the message. It shows that how the network card works. Here, the user can directly send the reply after seeing the information. Another type is that the person quietly watches everyone’s conversation and gets the wanted data and password with the help of a sniffer.

Recovery Mechanism

The sniffer is detected by the network experts. There are two possible ways to find the sniffer in the system, one way is physical checking of the system for the sniffer and another way is a software detection program, with the help of the program, the network device for the sniffer can be scanned efficiently. To protect information from sniffing, encryption technique, secure socket layer-protected websites and some protection tools have to be used.

E. Keyloggers

It is a technique based on password hacking. The hacker follows the Keyloggers technique in order to hack the username and password of the user. The hacker made the user to install the software so that the hacker can easily hack it or else the hacker itself installs the software that keeps all the logging activity specially the information typed by the user through the keyboard including username and password.

Recovery Mechanism

To avoid this before installing the software the users have to ensure that the software is trusted and belonged to the certified organization.

F. Shell Shock

The Shell Shock [4] exposure bears on Bash which is a program where as sorted Unix-based systems used to accomplish command lines and command scripts. This is many times at short intervals installed as the system's non remittal command line interface. Bash is autonomous software, formulated together and managed since 1992 on a volunteer basis by Chet Ramey who is a professional software architect. Synthesis of the source code chronicle of Bash shows the vulnerabilities had survived since version 1.03 of Bash which was released in September 1989, introduced by Brian Fox. Shell shock is also known as Bash door. It is of security glitch which is used mainly in Unix Bash Shell.

The web server distribution using the bash allows the attacker to cause assailable versions executing arbitrary commands in processing the requests. This makes an unauthorized access for the attacker. The commands are combined to the function definitions by the Bash caused by the bugs. These are laid aside in the values of environment variables. The Shell Shock [4] has been used to greatest advantage by the attackers by creating collection of computers controlled by the same malicious program which is used to carry out distributed act of refusing to someone’s rules with service attacks and the state of being vulnerable.

The security companies recorded millions of attacks and investigations related to the bug in the days following the disclosure. Shell Shock [5] with a possibility of becoming actual, compromise millions of unlatched servers and other systems. Because of the reasons given, it has been compared to the Heartbleed bug in its robustness. The initial list of environment variables for a program is provided by another. Apart from this, Bash also preserves an internecine list of functions named as scripts. These scripts are executed from within the program. It is accomplishable that the bash can be executed from within itself as it operates as a command interpreter and a command. By this time, the actual case can transfer the environment variable and function definition into the new instance. Function definitions are exported by encrypting them inside the environment multivariate list as variables whose values start with parentheses ("()") followed by a function definition. The new example of Bash, systematically examine its environment variable list for values in this specification and converts them back into internal functions. This conversion is performed by making a piece of code from the value and executing it, because of creating "on-the-fly". An attacker may execute arbitrary commands or manipulate other bugs that exists command interpreter.

Recovery Mechanism

To implement the cure for shellshock, organizations demand a way to evaluate their endpoint environment and then distribute systematically and manage the patches for the innumerous operating systems in their environment. An efficacious solution provides policy-based installation of security updates, closed-loop substantiation and the quality to manage patches transversely aggregate platforms from a single point of control. Shrivel patch deployment time to bring down the risks associated with Shellshock is experienced.

The attacks caused by this menace through its IBM Security Network, Intrusion Prevention product offering must be recognized and protected. The unparalleled focus on identifying and screening this vulnerability from an unsuccessful exploit, the clients were helped by the IBM to protect against these kinds of exploits since 2007. Remediating with the appropriate patch for the version of OS in which it is running.

III. Comparative analysis of hacking techniques

TABLE I. HACKING METHODS ANALYSIS

Hacking Techniques	Mode of Hacking	Technique Involved	Recovery Scheme	Processing Time
Heartbleed Bug	System Memory	OpenSSL cryptography	FixedOpenSSL	Normal
Man in the Middle Attack	Email Messages	ARP spoofing	HTTPS protocol with VPN access	Normal
POODLE	Encrypted Message	SSL 3.0	Controlling the usage of SSL	High
Sniffing	Network Address	Sniffer Codes	Socket layer protected websites	Normal
Keyloggers	Username & Passwords	Keyloggers technique	Certified Authentication	High
Shell Shock	Scripting Commands	Bash program	Intrusion Prevention	High

Thus the above Table 1 illustrates the several Hacking techniques issues and the techniques involved in it and thereby this comparison is not to inspect the best hacking technique but to help the readers as well as researchers in analyzing the recovery mechanisms.

Conclusion

Thus throughout this survey, several Hacking methodologies happening in the present scenario has been clearly specified. From this perspective, the user has the responsibility to perform authenticated methodology according to the impairment of each Hacking methods. The Comparative analysis of different hacking methods highly exemplifies the major mode of hacking along with the technologies involved behind it. Added to those corresponding recovery mechanisms to get rid of those harmful attacks has also been scrutinized effectively with the processing time. Henceforth this theoretical analysis will greatly helps the followers and various hackers as well as researchers to innovate more recovery solutions in future.

REFERENCES

[1] Bipin Chandra, “A Technical View of the OpenSSL Heartbleed vulnerability”White paper IBM, version 1.2.1, May 13 2014.

[2] R.Susmitha, D.Venkatasubramanian, R.Shyam Sundar, “Hacking methods, Techniques and their prevention”, International Journal of Computer Science and Information Technology Research, vol 2 issue 2, pp 183-189 June 2014

[3] PK Pateriya, “Analysis on Man in the Middle attack on SSL”,International Journal of Computer Applications, 45(23) May 2012.

[4] http://en.wikipedia.org/wiki/Shellshock_vulnerability

[5] http://security.stackexchange.com/questions/68448/where-is-bash-shellshock-vulnerability-in-source-code

[6] U.Nanaji, K.T.Makesh Babu, P.Sai Sampath, “Website Hacking: SQL Injection Method and its prevention”, International Journal of Computer Trends and Technology, vol 4, issues 4 April 2013.

[7] https://en.wikipedia.org/wiki/POODLE