International Journal on Recent and Innovation Trends in Computing and Communication
Volume: 4 Issue: 4

ISSN: 2321-8169
723 - 725

Cybercrimes and Attacks for Data access, Online Transaction with Overview of Cyber Security Acts

Asha Khatri
Department of Information Technology
K. J. Somaiya College of Engineering
Vidyavihar, Mumbai

Riya Savla
Department of Information Technology
K. J. Somaiya College of Engineering
Vidyavihar, Mumbai

Ayushi Malde
Department of Information Technology
K.J.Somaiya College of Engineering
Vidyavihar, Mumbai

Prof. Dipti Pawade
Assistant Professor, Department of IT
K.J.Somaiya College of Engineering
Vidyavihar, Mumbai

Abstract**—** The involvement of communication channel and/or communication network to commit a crime defines cybercrime. The uses of these systems are increasing in every work sector along with the risk and warnings which could affect individually or to a community. To overcome this issue people should know what it is and how it works. This paper gives information about cybercrimes, cyber laws for the offence, few attacks and their mitigation and a preventive tool Honeypots.

Keywords*- Cybercrime, IT ACT 2000, Salami, Linearization, Software Reverse Engineering, Honeypots***.**

*****

I. Introduction

Cybercrimes are the crimes that involve computers or networks as an object or tool to commit an offense. With the increasing number of use of computer the cybercrime is also increasing. Cybercrime security includes the tools you can use to safeguard your identity and assets in the online and mobile world. These tools can be anti-virus software, biometrics, and Web services and secure personal devices you carry with you every day. [1]

II. Cyber Law: IT Act 2000

The area of the computer and internet crimes are not only limited to identity theft or computer hacking, but also includes data processing, accessing without valid authorization and more. Countries around the world have laws that give potential penalties and punishments depending on the type of criminalised behaviour.

The Information Technology Bill was passed by both the houses of the Indian Parliament in May 2000. For e-commerce in India, this act seeks to deliver a legal framework. The cyber laws have a major impact for e-business and the economy in India. Therefore it is necessary to know what the different lookouts of the IT Act 2000 are and what it offers [8]. In table 1, few offences with their penalty under IT ACT 2000 are given.

III. Today's Cyber Security

Cyber Security can be provided using passwords, smart-cards or biometrics. Setting passwords is the most commonly employed mechanism by organisations. To serve the purpose user have to select strong password which is difficult to hack. But normally password provides the purpose of something you know. Since something you know can be easily known to anyone. Other way to ensure security is through something you have, which is served using smart cards. Even something you have can also be stolen, a combination of something you have and something you know is used, best example is Debit card. The Other way to ensure digital safety is using biometrics like face recognition, fingerprint recognition, iris recognition, retina recognition, etc.

TABLE I. IT ACT 2000

Section	Offence	Penalty
65	Tampering with computer source documents	Imprisonment up to three years, or/and with fine up to Rs 200,000
66	Hacking with computer system	Imprisonment up to three years, or/and with fine up to Rs. 500,000
66B	Receiving stolen computer or communication device	Imprisonment up to three years, or/and with fine up to Rs100,000
66C	Using password of another person	Imprisonment up to three years, or/and with fine up to Rs 100,000
66D	Cheating using computer resource	Imprisonment up to three years, or/and with fine up to Rs 100,000
66F	Acts of cyber terrorism	Imprisonment up to life.
67C	Failure to maintain records	Imprisonment up to three years, or/and with fine.
68	Failure/refusal to comply with orders	Imprisonment up to three years, or/and with fine up to Rs 200,000
69	Failure/refusal to decrypt data	Imprisonment up to seven years and possible fine.
70	Securing access or attempting to secure access to a protected system	Imprisonment up to ten years, or/and with fine.
71	Misrepresentation	Imprisonment up to three years, or/and with fine up to □100,000

Biometrics provides best way of ensuring security but due to high cost involved in authentication through biometrics they are not more widely used.

IV. Cyber Attack

Here we have discussed the threats that our computer or network is vulnerable to.

A. *Salami Attack*

Salami attack is a chain of activities which individually has negligible impression but when repeated many times results in powerful impact.

Salami attack is mostly performed by the insider of a firm who has access to network resources; the attacker can also be anonymous who may target the websites which stores account information like PayPal. The victims who fall over this attack are primarily bank holders and people using websites for accomplishing transactions.[2]

B. *Linearization Attack*

Most of the systems authenticate the user's digital identity with the help of passwords. On the backend if this password is checked one character at a time then this condition can be exploited to cause Linearization attack. Basically this attack is based on the principle that correct password will take more time for processing than the wrong password. The attacker can change one character at a time and on the basis of processing time, he can fix the correct character. This is how one by one attacker can retrieve the complete password for getting authenticated.

Linearization attack requires less efforts as compare to exhaustive brute-force attack hence is mostly used by attackers to gain access to data.[2]

C. *Software Reverse Engineering (SRE)*

It is also known as reverse code engineering. It can be utilized for both good as well as not so good purposes. Its good usage can be for understanding malware or legacy code of software. Here we will emphasize more on not so good uses which includes breaking Digital Rights Management systems, finding and exploiting software flaws, removing restrictions on usage of software and proprietary digital content among many others. SRE is very tedious and labour-intensive attack. It requires various expensive tools and a very skilled, intelligent and patient attacker. The SRE attacker must have knowledge of assembly coding.

The SRE attacker only has .exe file and no source code. The attack needs to accomplish his task through exe file only. No doubt, once the attack is successful the gain from the attack is worth more than efforts put in. The tools used for SRE are as follows:

1) Disassembler: - It converts .exe to assembly code. But there is no assurance that assembly code provided is always correct. It only gives static view of program logic.

2) Debugger: - It helps to give dynamic view of assembly code. It sets break points which helps attacker to better understand which instruction is meant for what. E.g. Soft slice, OllyDbg.

3) Hex-Editor: - It is used to patch i.e. make changes to exe file to modify its behaviour. Once the attacker is capable of doing that the software will behave according to attacker. E.g. Ultra Edit, HIEW [2]

V. POSSIBLE MITIGATIONS

A. *Solution For Salami Attack*

It has been observed that Salami attack is most common in banking sector. From bank customer point of view, keeping their eyes open is the most promising solution for Salami attack. Everyone needs to be vigilant about every bank transaction. Any deduction might be small (few paise) or big (in hundreds or thousands) should be reported to the bank. So that they can investigate their system. From banks part, continuous security updates are expected.

Banks as well as customer should avoid information sharing over the insecure network. [2]

B. *Solution For Linearization Attack*

- Having a multiphase-authentication system.
- Using cryptographic techniques to store password in database instead of raw password.
- Passwords being most vulnerable means of authentication, use of other means of authentication such as biometrics, smart-card or combination of them to gain access to highly sophisticated systems is advised.[2]

C. *Solution For Software Reverse Engineering*

- Anti-disassembly techniques: Use of bogus instructions to confuse disassembler. But a clever attacker can figure it out.
- Anti-debugging techniques: We can monitor for use of debug registers and insertion of breakpoints. Use of interactive threads may confuse debugger. Again, clever attacker will figure this out.
- Tamper-resistance: The goal is to make the patching of exe file difficult. Here, the code can hash parts of itself.
- Code Obfuscation: The goal here is to make understanding of code more difficult.

SRE is the most serious kind of attack that don't have a full-proof solution until now. The above mentioned mitigations will just try to make attackers job more difficult but can't help to avoid SRE completely[2].

VI. Preventive Tool: Honeypots

Honeypots can be used to analyse activities of attacker trying to access our network. It can be used as security surveillance tool.

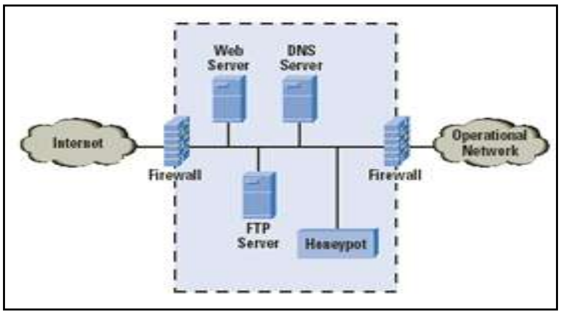

Figure 1. Honeypot attack

The main advantage of using honeypot is that it gives the caveat well in advance. This results into considerable decrease in risk of attacks over network. Apart from that it has an ability to scrutinize vulnerabilities. We know that in digital security if we safeguard ourselves against any attack, then the attacker come up with even more alarming attack. In this situation to mitigate an attack honeypots can serve as a best tool to understand such occurrences and thus help the developers to come up with a solution[3]. The honeypots can be classified as

- Pure
- Low interaction
- High interaction

1) Pure Honeypots

Here trap has been mounted on honeypot link to the network. It keeps watch on various activities of attacker so that if anything goes wrong will be caught immediately. Pure honeypots are considered to be the complete system which does not require extra software installation.

2) Low Interaction Honeypots

Low-interaction honeypots simulate only the services frequently requested by attackers. Since they consume relatively few resources, multiple virtual machines can easily be hosted on one physical system. . Example: Honeyd.[3]

3) High Interaction Honeypots

High-interaction honeypots imitate the activities of the production systems that host a variety of services and, therefore, an attacker may be allowed a lot of services to waste his time. By employing virtual machines, multiple honeypots can be hosted on a single physical machine. Therefore, even if the honeypot is compromised, it can be restored more quickly.

Pros:

- ➢ More secure.[3]

Cons:

- ➢ Expensive to maintain.

B. Advantages And Disadvantages

Honeypots have their advantages and disadvantages. They are clearly a useful tool for luring and trapping attackers, capturing information and generating alerts when someone is interacting with them. The activities of attackers provide valuable information for analysing their attacking techniques and methods.

However, honeypots do have their drawbacks. Because they only track and capture activity that directly interacts with them, they cannot detect attacks against other systems in the network. Furthermore, deploying honeypots without enough planning and consideration may introduce more risks to an existing network. Honeypots are designed to be exploited, and there is always a risk of them being taken over by attackers to gain entry to other systems within the network. This is perhaps the most controversial drawback of honeypots.[6]

VII. Conclusion

This is the time when the use of internet with computers and network is at its peak and growing immensely. Various algorithms and keys are used to maintain tight security. Despite all this attacker will be successful doing breaches because at the most we can try to mitigate attacks, making attackers job more difficult. Thus we can conclude that the awareness of cybercrime should be made known to every common man along with the laws, the various attacks and its mitigation. Also to use a tool like honeypots to prevent, detect and react to cyber-attacks.

References

[1] https://www.techopedia.com/definition/2387/cybercrime

[2] www.justaskgemalto.com/us/what-digital-security

[3] http://www.university.youth4work.com/JIT_Jawaharlal-Institute-of-Technology/study/4290-cyber-security

[4] http://alchetron.com/Honeypots-1420-W

[5] https://www.anomali.com/blog/mhn-modern-honey-network

[6] http://www.cs.sjsu.edu/~stamp/CS166/my_pdf/4_Software.pdf

[7] https://zeltser.com/modern-honey-networkexperiments

[8] https://en.wikipedia.org/wiki/Information_Technology_Act,_2000

[9] http://www.cyberlawsindia.net/Information-technology-act-of-india.htm