A Literature Survey:Why Attacks are Successful on Information Systems

Sumit Sharma, Anurekh Kumar, Shobha Bhatt[1]
Students (M.tech-IS), Assistant professor (CSE)[1]
AIACTR,Geeta colony, Delhi

Abstract- **In today's Life, Internet technologies are widely adopted. These technologies allow us to make our life simple and excited. At the same time, these technologies attract the attackers to do illegal things. Attackers break the users privacy and harm them financially and economically. In this paper, we have focused on the issues related to information security in internet technologies, strategies of attackers, reasons behind success of attacks.**

Index Terms-Confidentiality, Availability, Integrity, Interception, Modification, Fabrication, Interruption.

I. Introduction

Day by Day, new technologies are coming in existence and old one growing regularly which are making our life simple and excited. With the growth of these technologies, attackers focus is also increasing towards it. Today, awareness about the information security is not available as much as required. Most of the users do not know about the basic security features and tools so, they are becoming easy target of attackers.

In this paper, We focus on the main attacks which are possible. We will study about the types of attackers and their strategies of attacking. Finally, We will study about the awareness of the internet users about the basic security features and tools.

II. Attacks and their types

For secure communication, It is compulsory to maintain confidentiality, availability and integrity of information or data. These three basic terms combine to make CIA triangle, that deals with basic requirement for secure communication of information or data.

ISSN: 2278 – 7798

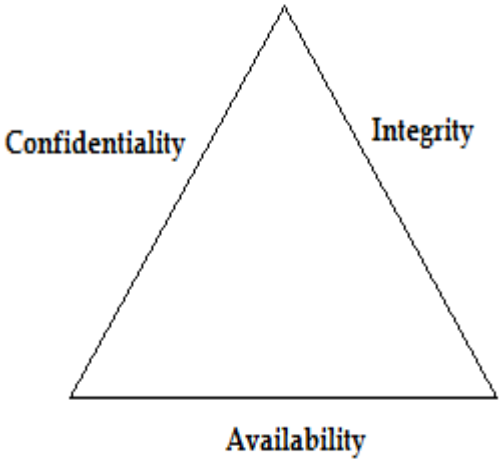


figure 1: Security Features

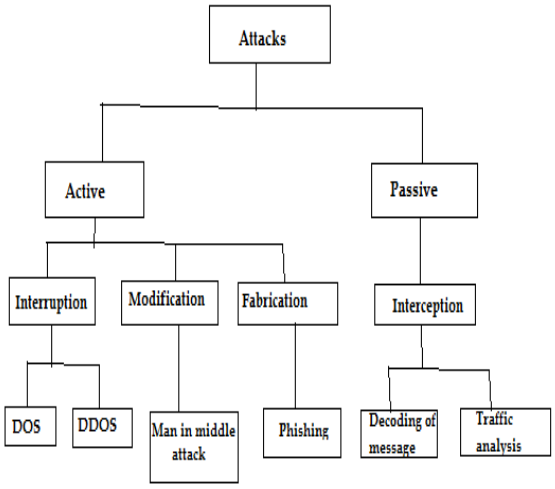


figure 2: classification of attcks

Confidentiality provides security from an unauthorized access to the data. Integrity provides that modification of data is only done by authorized user. Availability provides that data should be available when needed. The actual aim of attackers is to exploit CIA triangle.

An attack is an event where an unauthorized person gains access to the confidential data of the users. According to the nature of attacks, they classified in two categories, one is active attack and second is passive attack. An active attack is an attack where attacker changes or modify the content of the message or data whereas passive attack is an attack where attacker gets the confidential data or message content without any modification. Further active and passive attacks classified as shown in figure 2.

Active attacks are classified into three sub-categories which are Interruption, Modification and Fabrication. Interruption means interrupt or hide the data when needed. Interruption is provided by delaying or losing the data. Interruption is done through Denial of service attack (DOS) and distributed Denial of service attack (DDOS). In these techniques, attacker increasing the traffic on the server by which services of the server interrupted temporarily or permanently and data does not available when needed. Modification is the term whose means changing the content of message or data. It is done through different techniques in which one is man in middle attack. In it, attacker presents in between of the two users who communicate to each other. When one user sends data to second user then attacker collects it and sends modify data to the second user. Similarly, when second user sends data to first user then attacker collects it and sends modify data to the first user. Fabrication means making fake objects that looks like as actual

ISSN: 2278 – 7798

objects. Main intension of attacker behind it to collect important credentials of the users by making them fool. It is done through different techniques in which one is phishing. In it, attacker makes fake web-pages when user fill their important credentials on that page then it redirect user to actual page and sends users information to the attacker.

Passive attack are done by Interception. Here, main intension of attacker is to read the content of message or data. It is done through two techniques, one is Decoding of message and second is Traffic analysis. In Decoding of message, attacker guesses the content of message by making different possible combinations on the received data. In Traffic analysis, attacker monitors the all communication of the targets and collect important information then attacker uses guessing technique to find different possible combinations.

In the next figure we showed that which attack break which security feature.

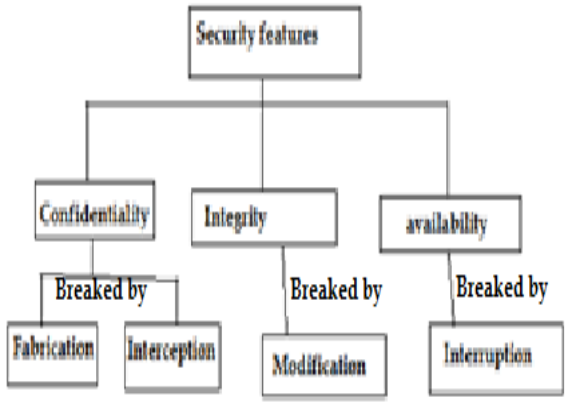


figure 3: attacks corresponding to security features

Now, we discuss about the framework which is used in data communication and the attacks possible on different layers of that framework. We have different models for data communications in which one is ISO-OSI (Open System Interconnection) model. It has complete structure and have seven layers. It is developed by International Organization of Standardization. It shows seven layers which involves in communication of any data. Each layer has its own work. In next table we show Responsibility and work of each layer.

Layers	**Responsibility and work**
Application layer	Interface between user and system
Presentation layer	Encryption and Decryption of data
Session layer	Managing user session
Transport layer	End to end communication
Network layer	Routing of data
Data Link layer	Error correction and Detection
Physical layer	Defines transmission properties of data

Table 1: Layers and their Responsibilities & work.

At Application, Presentation and Session layers attacks like viruses, worms and data corruption are possible. Viruses and worms are the self replicating programs that can affect the files presented in the system. At transport layer UDP/TCP synchronization is possible. At Network layer modification is possible. At Data Link

ISSN: 2278 – 7798

layer Interception is possible whereas at physical layer Eavesdropping is possible. In eavesdropping , attacker listens the call of users by showing that he or she is the actual receiver. Attacks possible on different layers are shown in following figure.

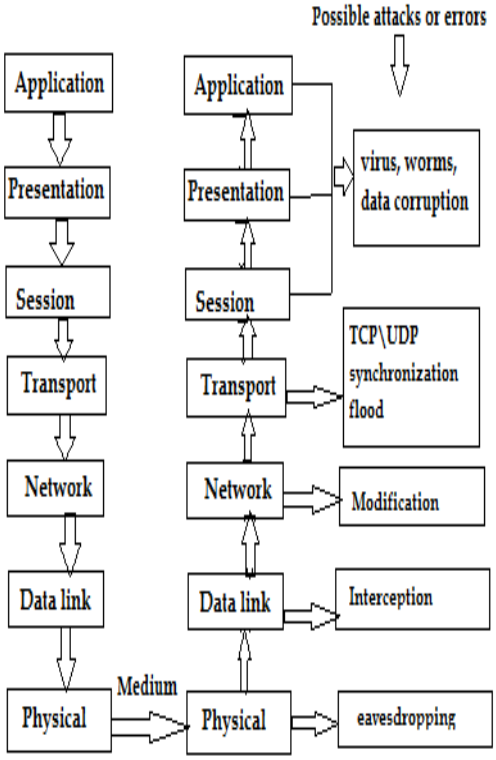


Figure 4: Network layers and corresponding attacks

III.Attackers and their Strategies

Attacker is the person who initiate the attack for stolen the important information about the target. Attackers are of three types which are White Hat hacker, Black Hat hacker and Grey Hat hacker.

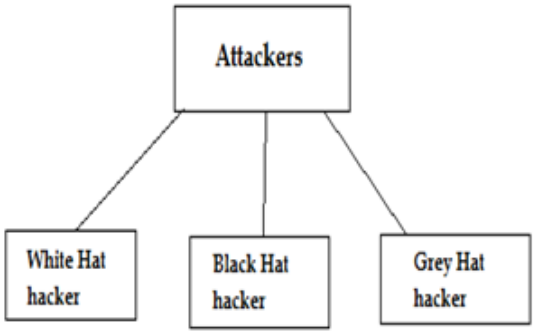


Figure 5: types of attackers

White Hat hackers are the legal attackers those having certificate for hacking. They find the threats and vulnerabilities presented in the system and softwares. Black Hat hackers misuse their skills for doing illegal activities. They take advantages of threats and vulnerabilities presented in the system for harming the financially and economically the target. Grey Hat hackers are the attackers, who takes the advantage of the situation and can do illegal activity.

Attackers make a strategy before actual attacking the target. These strategy can be divided into four phases. Each phase has its own importance and output. These phases can be iterative and cyclic in nature.

Phase 1:

In this phase attackers collect the important informations about the target. Attackers collect all relevant informations that can be helpful for actual attack. Attackers try to collect informations like infrastructure of target, software and hardware used by target, resources used by the target ext. After collecting such

ISSN: 2278 – 7798

information, attackers make a report which is helpful for actual attack.

Phase 2:

After making report about the target, attackers do actual work. They select tools for attacking and try to gain access to the target. In this phase, attackers try to enter in the system by using techniques like password cracking, dictionary attack ext.

Phase 3:

After gaining access, attackers main task is to do illegal work for which they attacked. In this phase, attacker changes the target system privileges so that, they could gain as much as possible. Attackers create a backdoor by installing software like Trojan horses ext. to gaining easy access for next visit.

Phase 4:

This phase distinguish between good attacker and smart attacker. Smart attacker always want that no-one could easily finds about the attack. For this, attackers clear the log files presented in the target system. Attackers install some software before doing anything on the target which records the attackers activities. After performing their task, attackers can easily clear the log files by the help of these software and delete all evidence of their presence. Attackers strategy phases with output can be shown in figure 6.

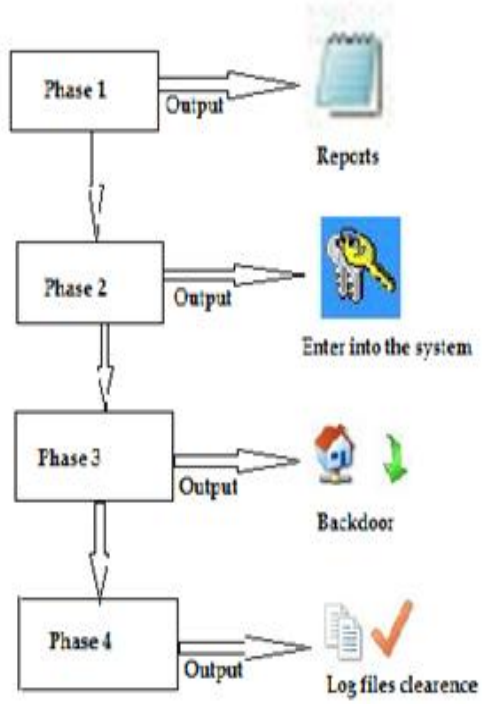
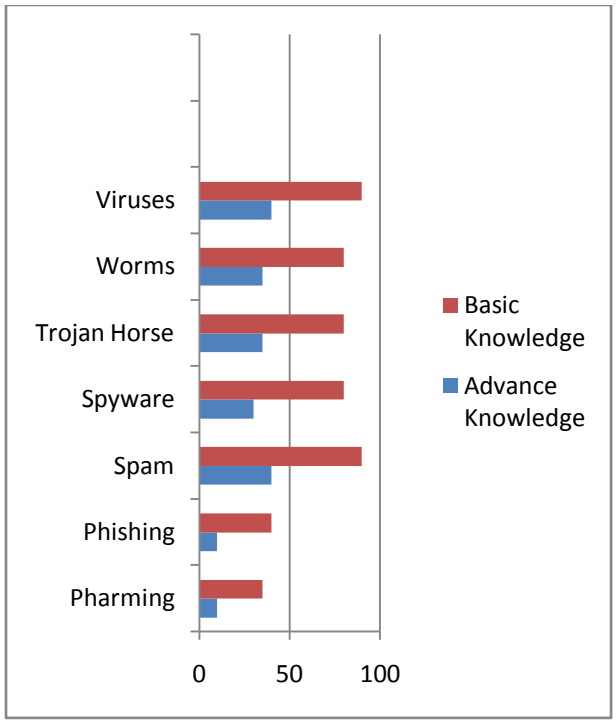


figure 6: Attackers strategies with output of each phases

IV.Why are the Attacks successful ?

The main question in our mind is that "Why are the Attacks successful ?". we tried to find out the answer of this question through a survey. We did a survey on the peoples having technical and non technical background and made a graphical record. First diagram shows the knowledge of peoples about the Harming techniques like Viruses, Worms, Trojan horse, Spywares, Spam, Phising and Pharming. We divided this survey in two parts, one is basic knowledge of peoples about Harming techniques and second is advance knowledge of peoples about Harming techniques.

ISSN: 2278 – 7798

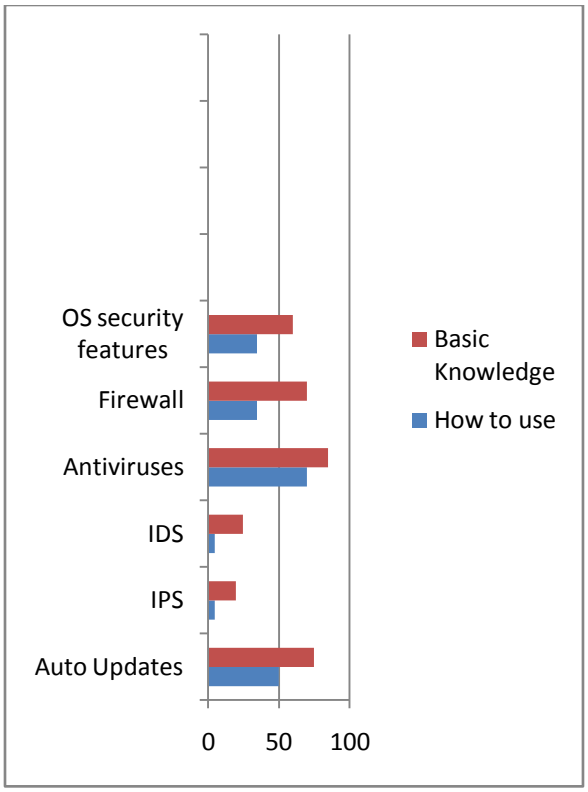


All data in %

From this survey we concluded that only 25% (average)[1] People knows about the mechanisms of these Harming techniques which is very less.

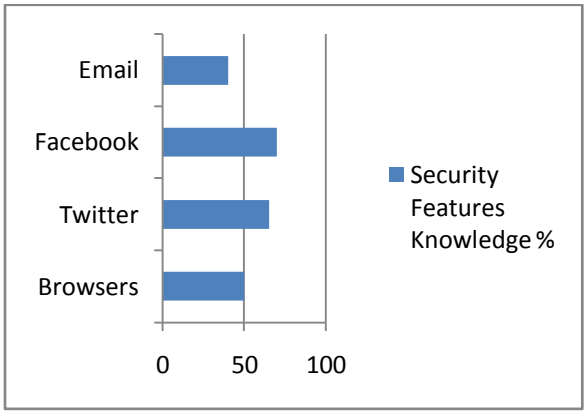
Second diagram of this survey shows that knowledge of people about the security features of Operating systems & other applications and security tools like firewall, Anti-viruses, intrusion Detection system (IDS), intrusion Prevention system (IPS). We concluded that most of the peoples do not know how to use these features and tools.

1. Average= (minimum value +maximum value)/2



All data in %

Third diagram shows that the knowledge of peoples about the browsers and social networking websites security features. We concluded that most of the users do not know about it.



ISSN: 2278 – 7798

Finally, we tried to find out answer of our question and concluded that lack of awareness of the internet users about the latest attacking techniques, security features of Operating Systems & other applications are the main reason behind the success of these attacks.

V. Conclusion

The main aim of this paper is to provide basic knowledge to the internet users about the attacks, attackers type and their strategies. In this paper, we tried to find out "Why are attacks successful ?" through a survey. This paper attract the internet users to know about attacks, attackers strategies, security features of the Operating systems & other applications and available security tools.

References

[1] Matt Bishop,2003, what is computer security?, IEEE.

[2] Zakaria Karim, Karim Mohammed Rezaul and Aliar Hussain,2009, towards secure information system in online banking, IEEE.

[3] Aviel D Rubin, Daniel E Geer jr., 1998, A survey of web security, IEEE.

[4] C. C. Palmer,2001, Ethical Hacking, IBM system journal vol 40 no. 3.

[5] Reto Banumann,2002, Ethical Hacking, GSEC practical version 1.4.

[6] Indian computer emergency response team,2004, Web server security guidelines, Department of IT, Ministry of communication and information technology, Govt. of India.

[7] Haoliang Zhang, Jinqiao Shi, Xiaojun Chen,2012, A multilevel analysis framework in network security situation awareness, International conference on IT & Quantitative management, Elsevier.

[8] S. M. Furnell, A Jusoh, D. Katsabas,2005, The challenges of understanding & using security: A survey of end-users, Elsevier.

[9] Atul Kahate,2004, Cryptography And network security, Tata Mcgraw Hill.

[10] William Stallings,2011, Cryptography And network security: Principles and Practice(5^{th} edition), Pearson.

[11] Behrouz A Forouzan,2004, Cryptography And network security, Tata Mcgraw Hill.

[12] Manideep K,2012, A complete practical guide to ethical hacking and information security, Scitech Publications.

[13] Ankit Fadia,2008, An unofficial guide to ethical hacking, Mac Millan Publisher.

ISSN: 2278 – 7798

Short Bio Data for the Authors

Ms. Shobha Bhatt has received her **M.E** degree in **Computer Technology & Application**. Her research interest encompasses internet technology and internet security. She has coauthored in various research papers published in various International journals and conferences proceedings. She is working as Assistant Professor in Department of Computer Science and Engineering of AIACT&R (Govt. of NCT of Delhi), geeta colony, Delhi.

Sumit sharma has received his **B.Tech** in **Information Technology** from HMR Institute of Technology & Management, affiliated to Guru Gobind Singh Indraprastha University, Delhi in 2012. He is pursuing **M.Tech** in **Information Security** from AIACT&R (Govt. of NCT of Delhi), geeta colony, Delhi, affiliated to Guru Gobind Singh University, Delhi. His area of interest encompasses internet security and cryptography.

Anurekh kumar has received his **B.Tech** in **Information Technology** from MAIT, affiliated to Guru Gobind Singh Indraprastha University, Delhi in 2011. He is pursuing **M.Tech** in **Information Security** from AIACT&R (Govt. of NCT of Delhi), geeta colony, Delhi, affiliated to Guru Gobind Singh University, Delhi., Guru Gobind Singh University, Delhi. His area of interest encompasses internet security and cryptography.

ISSN: 2278 – 7798