ANALYZING AND LISTING OF INTRUSION AND PEEPING ATTACKS OF HUMAN COMPUTER INTERACTION

[1]Deepanayaki M, [2]Anandhipriya S,
[1]Associate Professor, [2]II MCA Student
[1 2]Department of Computer Application,
Priyadarshini Engineering College, Vaniyambadi, Vellore, Tamilnadu, India

Abstract: The Human computer interaction system (HCI) is the study of how many people interacts with computers and to what extent computers are or are not developed for successful interaction with human beings. In this paper we proposed various types of peeping attacks such as Passive attack, Active attack, Shoulder surfing attack, and Web based attack.

IndexTerms*:* Active attack, shoulder surfing attack, passive attack, web based attack.

INTRODUCTION

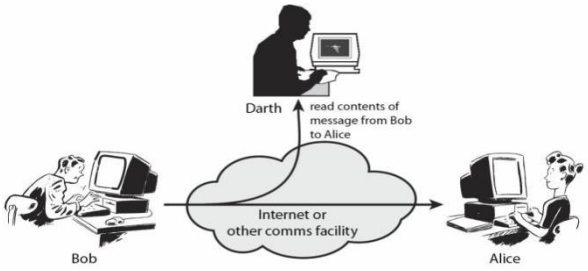
HCI deals with the interaction between more than one computer and more than one human. Research in HCI started focusing on improving the security and usability of software of through a systematic approach to design. Passive peeping attack can only passively monitor legal user's responses. Active peeping attacks adversaries control the communication channels and can disguise themselves as fake verifier. Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information. Web based attack focus on an application itself and functions on layer 7 of the OSI. This paper focuses on a special class of peeping attacks.

List of attacks

1. Passive(weak) peeping attack
2. Active(strong) peeping attack
3. Shoulder surfing peeping attack
4. Web based peeping attack

Passive (weak) peeping attack

A passive attack is a network attack in which a system is monitored and sometimes scanned for open ports and vulnerabilities. This purpose is solely to gain information about the target and no data is changed on the target.



Methods of passive attacks:

War driving

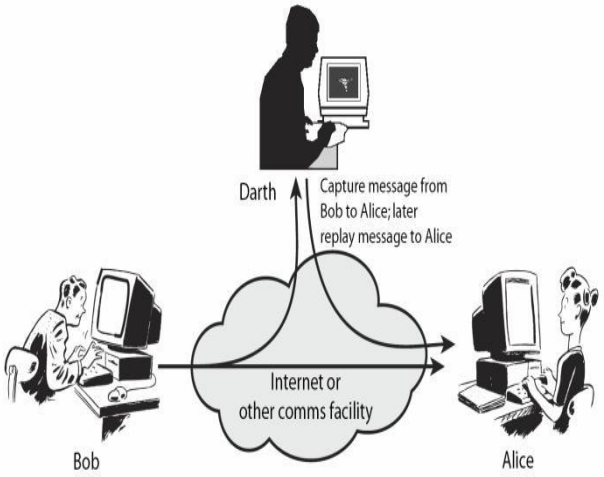
Detects vulnerable Wi-Fi networks by scanning them from nearby locations with a portable antenna.
The attack typically carried out from a moving vehicle, sometimes with GPS system that hacker use to plot out areas with vulnerabilities on a map.

Dumpster diving

In dumpster diving, intruders look for information stored on discarded computers and other devices or even passwords in trash bins. The intruders can then use this information to facilitate covert entry to a network or system. A passive attack contrasts or data en route for the target with an active attack, in which an intruder attempts to alter data on the target system system.

Active (strong) peeping attack

An active attack is a network exploit in which a hacker attempts to make changes to data on the target or data en route to the target.



Types of active attacks

1. Masquerade attack
2. Session replay
3. DOS
4. DDOS

1. In a masquerade attack, the intruder pretends to be a particular user of a system to gain access or to gain greater privileges than they are authorized.

A masquerade may be attempted through the use of stolen login IDs and passwords.

2. In session replay attack a hacker steals an authorized user's log in information by stealing the session id.

The intruder gain access and the ability to do anything the authorized user can do on the website.

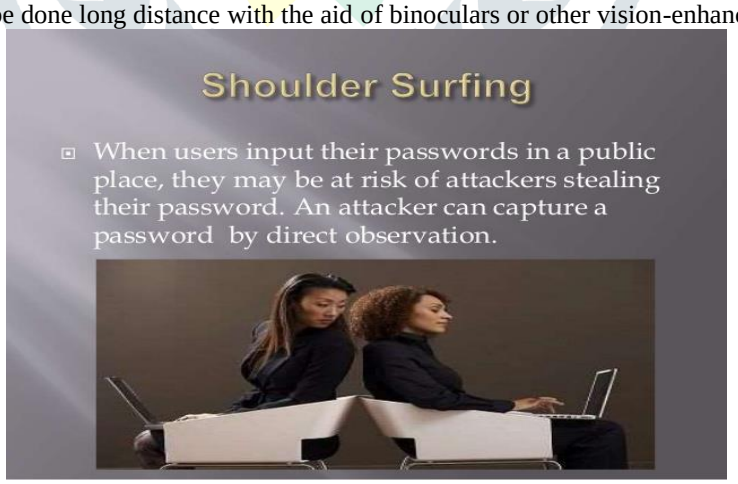
3) In a denial of service (DOS) attack, users are deprived of access to a network or web resource. This is generally accomplished by overwhelming the target with more traffic than it can handle.

4) In a distributed denial-of-service (DDOS) exploit, large numbers of compromised systems (sometimes called a botnet or zombie army) attack a single target.

Shoulder surfing attack

Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing is an effective way to get information in crowded places because it's relatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine, or us a calling card a public pay phone.

Shoulder surfing can also be done long distance with the aid of binoculars or other vision-enhancing devices.



Web based attacks

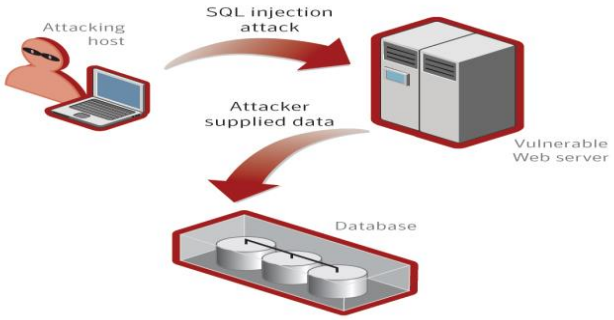
Web based attack are considered by security experts to be the greatest and often times the least understood of all risks related to confidentiality, availability, and integrity. The purpose of web based attack is significantly different then other attack; in most traditional penetration testing exercises a network or host is the target of attack. Web based attack focus on an application itself and functions on layer 7 of the OSI.

There are four types of a web based attack

> SQL injection attack
>Cross site attack
>Inclusion vulnerabilities: LFI&RFI
>Brute force attack

SQL Injection Attacks

Today many Web sites, particularly larger, high-traffic Web sites, serve up content that is dynamically constructed from information. Held in databases. As users interact with such sites, information is read from and written to the database. As a result of this, the task. Of securing the Web site must extend to the databases themselves, as Well as the data that is stored within them.



Cross site scripting (XSS)

Cross Scripting attack (XSS) is a types of computer security vulnerability typically found in web applications. XSS enables attackers to inject client-side script into web pages viewed by other users. A cross side scripting vulnerability may be used by attackers to bypass access controls such as the same origin policy.

File Inclusion vulnerability

File inclusion vulnerability is a type of vulnerability that is most commonly found to affect web applications that relay on a scripting run time.

There are two types of inclusion vulnerability,

RFI (Remote file inclusion)

LFI (Local file inclusion)

Brute Force Attack

A brute force attack is a trial-and-error method to obtain information such as a user password or personal identification number (PIN). In a brute force attack, automated software is used to generate a large number of consecutive guesses as to the value of the desired data.

CONCLUSION

In this paper we address danger of peeping attack in the real world and we introduce passive attack, active attack, shoulder surfing attack, and web based attack. A passive attack used to monitored and scanned for open port. Active attack is used to stolen login id and passwords. Shoulder surfing can also be done long distance with the aid of binoculars or other vision-enhancing devices. We hope in this paper can stir more further research on this subject research to lead the final success against peeping attack in Human computer interaction.

References

1. Shujun Li Heung-yeung Shum –Secure human- computer identification (interface) systems against peeping attacks: secHCI –Beijing 100080, China
2. Kayahan sayin-“Exploring HCI and security in instrusion” Universty of Birminghan
3. Triparna Mukherjee, Asoke Nath-“Securing Human computer intraction”-Kolkata, India
4. Andrew S. Partrick ,A Chris Long, Scott Flinn,”HCI and Security Systems” Canada