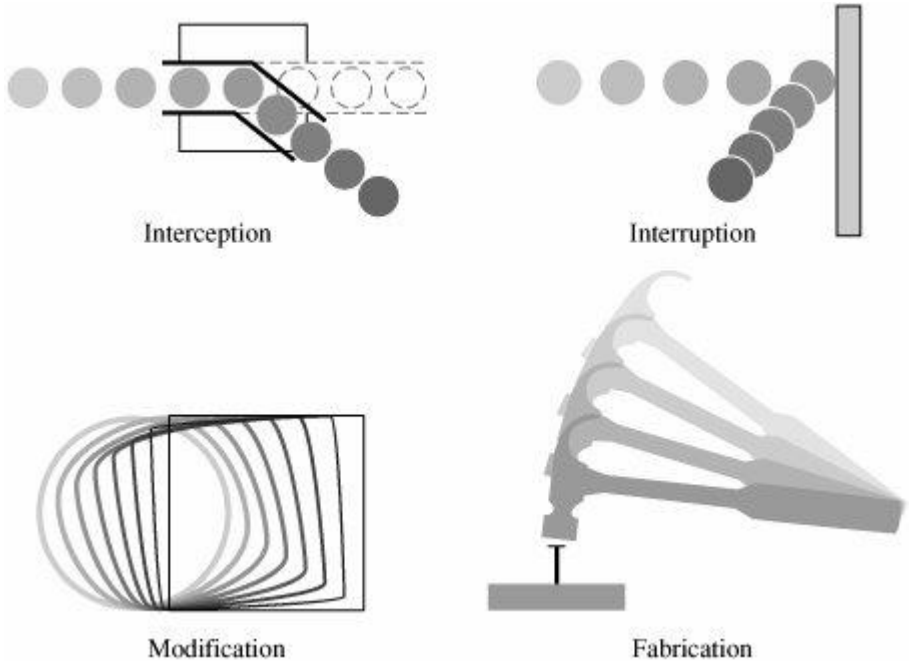
COMPUTER SECURITY

Unit –III

System Security-II: Interception, Interruption, Modification & Fabrication, Crackers & Career Criminals, Vulnerability & Abuses, Transient vs Resident virus, Control against threats, Password Management

Full details on types of threats can be read here.



- An **interception** means that some unauthorized party has gained access to an asset. The outside party can be a person, a program, or a computing system. Examples of this type of failure are illicit copying of program or data files, or wiretapping to obtain data in a network. Although a loss may be discovered fairly quickly, a silent interceptor may leave no traces by which the interception can be readily detected.
- In an **interruption**, an asset of the system becomes lost, unavailable, or unusable. An example is malicious destruction of a hardware device, erasure of a program or data file, or malfunction of an operating system file manager so that it cannot find a particular disk file.
- If an unauthorized party not only accesses but tampers with an asset, the threat is a **modification**. For example, someone might change the values in a database, alter a program so that it performs an additional computation, or modify data being transmitted electronically. It is even possible to modify hardware. Some cases of modification can be detected with simple measures, but other, more subtle, changes may be almost impossible to detect.
- Finally, an unauthorized party might create a **fabrication** of counterfeit objects on a computing system. The intruder may insert spurious transactions to a network communication system or add records to an existing database. Sometimes these additions can be detected as forgeries, but if skillfully done, they are virtually indistinguishable from the real thing.

COMPUTER SECURITY

Computer Security Attacks.

Interruption Attack
In an interruption attack, a network service is made degraded or unavailable for legitimate use. They are the attacks against the availability of the network.

Examples of Interruption attacks :
- Overloading a server host so that it cannot respond.
- Cutting a communication line.
- Blocking access to a service by overloading an intermediate network or network device.
- Redirecting requests to invalid destinations.
- Theft or destruction of software or hardware involved.

Mitigate the attack:
- Use Firewalls - Firewalls have simple rules such as to allow or deny protocols, ports or IP addresses. Modern stateful firewalls like Check Point FW1 NGX and Cisco PIX have a built-in capability to differentiate good traffic from DoS attack traffic.
- Keeping backups of system configuration data properly.
- Replication.

Interception Attacks :
In an interception attack, an unauthorized individual gains access to confidential or private information. Interception attacks are attacks against network confidentiality.

Examples of Interception attacks :
- Eavesdropping on communication.
- Wiretapping telecommunications networks.
- Illicit copying of files or programs.
- Obtaining copies of messages for later replay.
- Packet shiffing and key logging to capture data from a computer system or network

Mitigate the attack :
- Using Encryption - SSL, VPN, 3DES, BPI+ are deployed to encrypts the flow of information from source to destination so that if someone is able to snoop in on the flow of traffic, all the person will see is ciphered text.
- Traffic Padding - It is a function that produces cipher text output continuously, even in the absence of plain text. A continuous random data stream is generated. When

plaintext is available, it is encrypted and transmitted. When input plaintext is not present, the random data are encrypted and transmitted. This makes it impossible for an attacker to distinguish between tree data flow and noise and therefore impossible to deduce the amount of traffic.

Modification Attack

It is an attempt to modify information that an attacker is not authorized to modify. This type of attack is an attack against the integrity of the information. Basically there is three types of modifications.

- Change: Change existing information. The information is already existed but incorrect. Change attacks can be targeted at sensitive information or public information.
- Insertion: When an insertion attack is made, information that did not previously exist is added. This attack may be mounted against historical information or information that is yet to be acted upon.
- Deletion : Removal of existing information

Modifying the contents of messages in the network.

- Changing information stored in data files.
- Altering programs so they perform differently.
- Reconfiguring system hardware or network topologies.

Mitigate the attack :

- Introduction of intrusion detection systems (IDS) which could look for different signatures which represent an attack.
- Using Encryption mechanisms
- Traffic padding
- Keeping backups
- Use messaging techniques such as checksums, sequence numbers, digests, authentication codes

FabricationAttack :

In a fabrication attack, an individual inserts counterfeit information, resources, or services into the network. These attacks are attacks against the authentication, access control, and authorization capabilities of the network.

Examples of Fabrication Attack:

- Inserting messages into the network using the identity of another individual.
- Replaying previously intercepted messages.

- Spoofing a web site or other network service.
- Taking the address of another host or service, essentially becoming that host or service.

Mitigate the attack :

- Use of Authentication and authorization mechanisms
- Using Firewalls
- Use Digital Signatures - Digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document.

What is a computer cracker?

A computer cracker is an outdated term used to describe someone who broke into computer systems, bypassed passwords or licenses in computer programs, or in other ways intentionally breached computer security. Computer crackers were motivated by malicious intent, for profit or just because the challenge is there.

System crackers, often high school or university students, attempt to access computing facilities for which they have not been authorized. Cracking a computer's defenses is seen as the ultimate victimless crime. The perception is that nobody is hurt or even endangered by a little stolen machine time. Crackers enjoy the simple challenge of trying to log in, just to see whether it can be done. Most crackers can do their harm without confronting anybody, not even making a sound. In the absence of explicit warnings not to trespass in a system, crackers infer that access is permitted. An underground network of hackers helps pass along secrets of success; as with a jigsaw puzzle, a few isolated pieces joined together may produce a large effect. Others attack for curiosity, personal gain, or self-satisfaction. And still others enjoy causing chaos, loss, or harm. There is no common profile or motivation for these attackers.

Career Criminals

By contrast, the career computer criminal understands the targets of computer crime. Criminals seldom change fields from arson, murder, or auto theft to computing; more often, criminals begin as computer professionals who engage in computer crime, finding the prospects and payoff good. There is some evidence that organized crime and international groups are engaging in computer crime. Recently, electronic spies and information brokers have begun to recognize that trading in companies' or individuals'

secrets can be lucrative. Recent attacks have shown that organized crime and professional criminals have discovered just how lucrative computer crime can be. Mike Danseglio, a security project manager with Microsoft, said, “In 2006, the attackers want to pay the rent. They don’t want to write a worm that destroys your hardware. They want to assimilate your computers and use them to make money” [NAR06a]. Mikko Hyppönen, Chief Research Officer with the Finnish security company f-Secure, agrees that today’s attacks often come from Russia, Asia, and Brazil and the motive is now profit, not fame [BRA06]. Ken Dunham, Director of the Rapid Response Team for Verisign says he is “convinced that groups of well-organized mobsters have taken control of a global billion-dollar crime network powered by skillful hackers” [NAR06b].

Computer cracker vs. hacker

The antiquated phrase *computer cracker* is not used anymore. It was originally proposed as an antonym, or the opposite, of the term *hacker*. Hacker initially applied to only those who used their computing skills *without* malicious intent -- they broke into systems to identify or solve technical issues. Skillful technologists with altruistic motives were called *hackers*; those with bad intent were called *computer crackers*. This distinction never gained much traction, however.

In 1993, the Internet Users' Glossary defined hacker as "a person who delights in having an intimate understanding of the internal workings of a system, computers and computer networks in particular. The term is often misused in a pejorative context, where 'cracker' would be the correct term."

The Glossary defined a computer cracker as "an individual who attempts to access computer systems without authorization. These individuals are often malicious, as opposed to hackers, and have many means at their disposal for breaking into a system."

The term *computer cracker* was subsequently subsumed by the term *black hat*, another outdated term for threat actor.

COMPUTER SECURITY

It should be noted, however, that people today rarely distinguish between ethical hackers and malicious hackers. Although hackers, by definition, do not have malicious intent, some people assume malicious intent when the word is used in everyday context.

Vulnerability & Abuses

Vulnerabilities are weaknesses in a system that gives threats the opportunity to compromise assets. All systems have vulnerabilities. Even though the technologies are improving but the number of vulnerabilities are increasing such as tens of millions of lines of code, many developers, human weaknesses, etc. Vulnerabilities mostly happened because of Hardware, Software, Network and Procedural vulnerabilities.

1. Hardware Vulnerability:
A hardware vulnerability is a weakness which can used to attack the system hardware through physically or remotely.
For examples:
1. Old version of systems or devices
2. Unprotected storage
3. Unencrypted devices, etc.

2. Software Vulnerability:
A software error happen in development or configuration such as the execution of it can violate the security policy. For examples:
1. Lack of input validation
2. Unverified uploads
3. Cross-site scripting
4. Unencrypted data, etc.

3. Network Vulnerability:
A weakness happen in network which can be hardware or software.
For examples:
1. Unprotected communication
2. Malware or malicious software (e.g.:Viruses, Keyloggers, Worms, etc)
3. Social engineering attacks
4. Misconfigured firewalls

4. Procedural Vulnerability:
A weakness happen in an organization operational methods.
For examples:
1. Password procedure – Password should follow the standard password policy.

2. Training procedure – Employees must know which actions should be taken and what to do to handle the security. Employees must never be asked for user credentials online. Make the employees know social engineering and phishing threats.

What Is Computer Abuse?

Computer abuse is the legal term for the use of a computer to carry out improper or illegal activities, but which do not constitute financial crimes that would be classified as wire fraud.

Examples of computer abuse include using a computer to expose personally identifiable information (PII) such as Social Security numbers, using a computer to change the content of a website owned by someone else, intentionally infecting one computer with a virus or worm that will spread to other computers, using a computer to illegally share copyrighted items, or using one computer to gain unauthorized access to another. Other examples of computer abuse include cyber bullying and using a work computer for personal tasks on company time.

Computer abuse arises from the use a computer to harm somebody else in some way. People who commit computer abuse may be violating company policies, university policies, or federal law. Responding to computer abuse involves identifying the offending computer(s) and then trying to identify the individual abuser(s).

Some definitions of computer abuse consider computer crime to be a type of computer abuse. Other definitions consider the two to be completely distinct, calling computer abuse something dishonest or unethical and computer crime something illegal. These opinions are irrelevant; however, when it comes to the federal law governing computer abuse: The Computer Fraud and Abuse Act of 1984 (CFAA)

Virus

There are many kinds of viruses. Viruses come in a wide variety. The level of destructiveness of viruses varies widely. Virus behavior can range from annoying to destructive. Viruses can be divided into two types: transient or resident.

Transient Virus: A Transient virus has a life that depends on the life of its hosts; the virus runs when its attached program executes and terminates when its attached program ends.

Resident Virus: A Resident viruses do not search for hosts when they are started. Instead, a resident virus loads itself into memory on execution and transfers control to the

host program.
The virus stays active in the background and infects new hosts when those files are accessed by other programs or the operating system itself.

Control against threats

1. Security policy first

At a minimum, your security policy should include procedures to prevent and detect misuse, as well as guidelines for conducting insider investigations. It should spell out the potential consequences of misuse.

Start by reading through your existing security policies, especially those regarding incident handling. Rework sections that rely on trusting insiders. For example, your incident-handling plan shouldn't require your team to contact the administrator of a suspect system to gain access; he or she may be the culprit.

Next, make sure that your policy details the limits on access to and dissemination of personal data about your employees, temps and others who might be targets of investigations. Mishandling this data can have severe consequences, including legal action. Specify who is allowed to access what data, under which circumstances, and with whom they are allowed to share this information.

Finally, to protect the organization from allegations of unfair or unequally applied penalties, make sure your security policy spells out the consequences of misusing company resources.

2. Don't neglect physical security

Regardless of whether you "own" physical security, consider it your No. 1 priority. Simply keeping people away from your critical infrastructure is enough to prevent most insider incidents.

Consider what happened to Red Dot, a Seattle-area heating and cooling company, where two janitors combed through garbage cans, desks and filing cabinets, stealing employee

and customer personal information. They obtained fraudulent credit cards and illegally accessed bank accounts, stealing tens of thousands of dollars before they were arrested.

Isolate high-value systems in restricted areas, and apply tight access control. You may be tempted to rely on keycards -- they're flexible and inexpensive -- but they're only single-factor authentication and can be lost, stolen or borrowed. The audit log may show that Alice entered the computer room at 10:03:34 a.m., but what if it was really Bob using her key?

Two-factor authentication -- for example, using a PIN and a keycard -- to augment keycards will thwart card thieves, but obliging employees will still loan their cards and PINs to colleagues.

Consider biometric authentication. Fingerprint scanners and similar devices are popular, albeit expensive choices.

But securing your computer systems isn't enough. Thieves, or overly curious colleagues, will grab sensitive information from unsecured hard copy. Make sure all your employees have at least one lockable drawer in their desk or file cabinet for securing sensitive information.

3. Screen new hires

In general, the more time you spend investigating an applicant's background, the better. If your organization considers background checks too time-consuming, consider outsourcing.

Background checks don't always tell the whole story, however. For example, a typical check might verify the applicant's current address, but would fail to reveal that someone living at the same address is a known con artist or a disgruntled ex-employee.

Services such as Systems Research & Development's NORA (Non-Obvious Relationship Awareness) can find such relationships. By combining information from seemingly

unrelated corporate databases, NORA can perform personnel checks -- on employees, subcontractors and vendors -- as well as prospective hires.

4. Use strong authentication

Passwords are passé. Password-cracking technology is quite advanced, and stronger passwords spawn forests of Post-it notes on monitors. And many employees share passwords.

The alternatives are expensive, and general deployment is beyond the means of most organizations. A more cost-effective compromise is to apply strong multifactor authentication only to particularly sensitive applications or systems, such as HR or accounting.

If you do deploy multifactor authentication -- combining user IDs and passwords with tokens, smart cards or fingerprint readers, etc. -- be aware that these methods may not plug all the holes. Once your session is established, a knowledgeable insider may be able to spoof new transactions under your name or simply use your computer while you've stepped away. Windows stations can be set to lock out users after a fixed period of inactivity and require reauthentication.

5. Secure your desktops

You can't depend on users to be responsible for all their configurations, but if you're using Microsoft's Active Directory service, you can use group policies to lock down desktops across your enterprise.

Group policies allow a security manager to set configuration details for the OS and its components (Internet Explorer, Windows Media Player, etc.), as well as other apps. For example, you can change the settings for each of Internet Explorer's security zones, enforce the use of your organization's content filtering internet proxy and even forbid the use of unsigned third-party macros in Microsoft Office apps. Windows itself comes with a number of sample template files, and more are available from Microsoft's website or

from the Windows or Office Resource Kits. In addition, make sure access rights to network folders are applied on a strict need-only basis.

6. Segment LANs

Host- or network-based intrusion detection systems deserve a prominent place on the roster of your internal defenses, but finding good monitoring points can be challenging.

Host-based systems usually deploy agents, but network-based systems rely on LAN sniffers. Monitoring a single internet connection is easy, but finding good locations -- choke points -- inside often-chaotic LANs can be more difficult. Ideally, you'd have one sniffer for each LAN segment. In a large network, this is unwieldy, impractical and will probably overwhelm you with worthless alerts.

A better tack is to treat your LAN as a series of enclaves, each of which comprises its own zone of trust, segregated by firewalls at the point where each connects with the corporate backbone.

7. Plug information leaks

Sensitive information can flow out of your organization through email, printed copies, instant messaging or by people simply talking about things they should keep to themselves. Combine security policy and technology to stanch the bleeding.

First, make sure your policy details restrictions on disseminating confidential data.

Technology can help, starting with the intrusion detection system (IDS). Scan your business plan for unique phrases that you wouldn't expect to find anywhere else and configure your IDS to alert you whenever it sees these telltale snippets on the network.

Email firewalls can scan the full text of all outgoing email.

Digital rights management tools restrict distribution of documents by assigning access rights and permissions.

8. Investigate anomalous activities

You probably collect reams of log data from your internet-facing servers: Unix syslogs, Windows event logs, firewall logs, IDS alerts, antivirus reports, dial-up access logs or any of a number of other different audit trails. But what about your internal LAN?

Unlike external attackers, insiders generally aren't careful about covering their tracks. "It's as if the attacker doesn't expect to be caught. Generally, none of the insider attacks we have seen were difficult to investigate," said Peter Vestergaard, former technical manager at Danish security consultancy Protego. "The biggest problem has been that companies don't have sufficient logging. In one case, almost no one knew that logging on a nondomain controller NT/Win2K server is disabled by default. Therefore, little or no log material was available."

Once you've got the log files, you're left with the often-difficult task of sorting through them for suspicious activity. "In all the noise, it's hard to identify a particular person trying to get information on the network," said an information security officer for a large U.S. insurance and financial services company, who requested anonymity. His company uses a home-brewed analysis engine that combines information from several different logs and looks for questionable patterns.

If you have the money, network forensic analysis tools can analyze the flow of information throughout your network.

9. Refocus perimeter tools and strategies

By applying your perimeter tools to the inside of your network, you can greatly increase your security posture, often at little cost. Step one is internal patching. You wouldn't dream of putting unpatched web or email servers on the public internet, so why should you settle for them on your LAN?

Step two is securing hosts by eliminating unused services and locking down configurations.

Once you've got the basics covered, you can add more external tools to your internal repertoire. If you're already using vulnerability assessment tools for your internet-facing services, scan your internal network for very little additional cost. Begin by scanning your most critical servers, like internal email, web and directory servers, then prioritize other systems and scan them in order.

10. Monitor for misuse

Your security may require direct Employee monitoring -- from video cameras to keystroke logging. Research suggests that as many as one-third of all employers perform such monitoring to some degree.

Before jumping on the bandwagon, though, make sure you know what tools are available to you and what constitutes legal monitoring in your jurisdiction.

Web content filters are useful tools, since they can be set to block pornography, competitors' websites and hacker tool repositories, all of which figure prominently in common insider security threats. In general, you can safely employ these as a matter of policy for all your workers.

If you need more detailed information about what specific employees are doing, you must exercise a bit more discretion, but you still have plenty of options that offer keystroke recording, application activity and window title logging, URL visit history and more.