OPERATING SYSTEM

Lecture 11

Operating System Security

Dr. Victoria Mukami

INTRODUCTION

This lecture focuses on operating system security. We will start by reviewing the role of the operating system in security. Specifically, we will look at system survivability, levels of protection, and backup and recovery. We will also look at security breaches and system protection.

Learning objectives

By the end of this topic, you should be able to:

1. Understand the role of the operating system in security
2. Identify the different types of security breaches
3. Understand system protection within a computer system

OVERVIEW

So far, all that we have done has been a culmination of this moment. We have reviewed the inner workings of the operating system including, memory allocation, processor management, device management, and file management. All this has been aimed at understanding how operating systems work to manage and control the computer. We now move on to operating system security. Security is key for any organism, computers included. Security within the English language is defined as a state of being free from any danger. Computer security on the other hand is the protection of computer systems from any threat. Threats in this regard can be unauthorized use, attacks on the computer, and harm toward the computer.

ROLE OF THE OPERATING SYSTEM IN SECURITY

The operating system plays a key role in computer system security. If the operating system detects a vulnerability, it is necessary for the operating system through the system administrator to guard against attacks. Within this section, we review system survivability, levels of protection, and backup and recovery.

System Survivability

Survivability talks about continuing to live or exist regardless of any hardships. System Survivability on the other hand talks about the capability of a system to fulfill its objectives regardless of any threats or attacks [1]. There are four properties of any survivable system. This includes [1]

1. Resistance to attacks
2. Recognition, when attacked including damage, inflicted
3. Recovery of essential services after an attach
4. Adaptation and evolution of system defense to stop future attacks

It is critical for any system to be able to fend off attacks from the very beginning. System survivability should not be an afterthought. Some strategies exist for each of the four properties discussed above.

Resistance to attacks: These strategies mainly feature ways or methods with which to stop attacks from occurring or from the system even being a target of attacks. Some ways of dealing with this are using authentication mechanisms, use of access controls, and encryption of information.

Recognition of attacks: These are ways in which the system can detect when an attack is imminent and if it occurs, evaluate the damage. Strategies for this include intrusion detection and integrity checking [1].

Recovery of services: These are strategies that involve a recovery of services that are essential for the computer to run especially after an attack. Strategies that exist include system backup and recovery, contingency planning, and data replication [1].

Reduction of future attacks: This focuses on strategies to prevent future attacks. This is a focus on increasing system survivability. A key strategy is the use of intrusion recognition patterns.

Levels of Protection

When a system is attacked and the attack is successful, the data within the computer can no longer be trusted [1]. Different computer configurations will have different ways in which their protection is done, the amount of risk they face, and specific vulnerabilities. Table 1 adapted [1] is a summary of the levels.

Table 1: Summary of Protection levels (Adapted [1])

TYPE OF CONFIGURATION	EASE OF PROTECTION	TYPE OF RISK	VULNERABILITIES
Single Machine - no network connection	High	Low	• Compromised passwords • Virus
Machine on the network - no internet access	Medium	Medium	• Spoofing • Sniffers • Compromised passwords • Viruses
Machine on a network with internet access	Low	High	• Email • Web servers • Sniffers • Spoofing • Compromised Passwords • Viruses

Backup and Recovery

Backup and recovery work on the premise that a user does not want to lose content if their system is compromised. Most administrators will schedule backups consistently to ensure that they can restore data and files without losing too much. The backups can be real-time (used for critical systems), hourly, daily, or weekly. Backups are encouraged to be conducted offsite to ensure a recovery plan especially when a disaster destroys the site. Existing policies on how the recovery will be conducted are also key to ensuring success.

SECURITY BREACHES

A breach is defined as breaking into something whether it is an agreement, a system, a house, etc. A breach occurs due to a vulnerability of some sort. These vulnerabilities can be intentional or unintentional. Consider forgetting to lock your house and a burglar breaks in and steals your electronics. This is an example of a breach. When we review system breaches, we are focusing on those that are malicious or not. In this section, we review intentional and unintentional security breaches.

Unintentional system attacks

These are system breaches that occur unintentionally i.e., there was no planned intrusion [1]. This can sometimes lead to an error. For instance, a process may modify a record and make changes without having the right permissions. This can lead to errors.

Intentional System Attacks

These are system attacks that include denial of service attacks, browsing, wiretapping, and trapdoors [1]. Think of intentional attacks because of someone performing malicious attacks. For instance, a disgruntled former employee may end up modifying files or even copying confidential files and taking them to a competitor.

Denial of Service Attacks (DoS): these are coordinated attempts that deny service to authorized users by making a computer perform a task repeatedly taking up resources that the user needs and making the computer unable to work.

Browsing: this happens when unauthorized users can get access to search through storage devices, directories, or files that they are not authorized to read [1].

Wiretapping: this is like what you see in movies where some branch of the police/military taps telephones to listen to a conversation. This is the same as an unauthorized user listening to a transmission being sent through a network without changing content.

Trapdoors: These are backdoors with which a hacker could gain access to a system. They are either a flaw in the system or are more likely installed by a system analyst to be able to maintain or debug a system [1].

Viruses

This is a small program that alters how a computer works without the knowledge or permission of the user [1]. Two criteria that determine if something is a virus

- Should be self-executing
- Should be self-replicating

A virus is usually written for a specific operating system. The person who creates the virus will look at the vulnerability in the operating system and target that vulnerability.

Some of the more famous more destructive viruses include the ILOVEYOU virus which caused approximately $10 billion in damage, Melissa which targeted and infected word documents and caused disruption online, and Zeus which targeted Windows machines by compromising user accounts. There are five main types of viruses [1]:

- File infector virus - infects executable files
- Boot sector virus – this infects the boot record within secondary storage
- Master boot records – this infects the boot record of a disk
- Multipartite virus – infects both the boot record and program files
- Macro virus – infects data files

Worms

A worm can propagate itself and therefore a user does not need to open any files for a worm to infect itself. The worm just copies itself from one system to the next. A worm makes a computer run slowly by taking processing time and memory space [1].

Adware and Spyware

Adware is an application that displays advertising banners while a different program is running. It gets downloaded automatically into a system while a user is browsing on the internet. It will pick information about a user's history, cookies, and other user-relevant information to deliver personalized advertising [1]. Spyware on the other hand is a program that is installed with or without a user's permission. The program will pick information about users such as websites visited, passwords, credit cards, and banking data [1].

Trojan

Ever watched the movie Troy or better yet read the Greek mythology on Troy? Well, Troy is a story where the Greeks received a gift of a horse that carried soldiers inside who were looking to breach the city of Troy. A computer trojan acts the same way. It masks itself as a legit program then goes ahead and starts copying information such as passwords.

SYSTEM PROTECTION

There are different ways in which one can protect a system. One does system protection to protect from outsiders and insiders. This is to ensure that there is no theft

of intellectual property or confidential information. There are three main methods of protection: installing antivirus, using firewalls, and encryption.

Antivirus protection

This is software that protects one's system from intentional attacks. Consideration of the type of data that needs to be protected will determine the type of antivirus software. The software can either be preventive or diagnostic. Preventive software prevents an attack while diagnostic software checks to make sure that none of the files is attacked.

Firewalls

This is either in the form of hardware or software that protects a system by masking its IP address to people outside of the system. A firewall is found between a network and the internet. A firewall has several tasks [1]

- Log any activities that access the internet
- Maintain access control based on the receivers IP address
- Maintain access control of the services required
- Hide the internal network from unauthorized users
- Verify that virus protection is installed and is working as should
- Perform authentication for any requests originating from the internet

Encryption

This is protection where data is encrypted. Encryption means putting data into a secret code [1]. Data is then communicated when in encrypted form while it gets decrypted on the receiving end.

SUMMARY

This lecture was a focus on operating system security. We reviewed the role of the operating system in security. Specifically, we looked at system survivability, levels of protection, and backup and recovery. Finally, we reviewed security breaches and system protection.

DISCUSSION TOPIC

Throughout this lecture, we have reviewed the ideas of security and how to secure an operating system. Now, do a review of the latest Windows operating system and highlight unique security features that were not present in past systems. Do a presentation of the findings to your instructor.

REFERENCES

[1] McHoes, A., & Flynn, I., Understanding Operating Systems. Boston: Cengage Learning, 2018

[2] Stallings, W., Operating Systems: Internals and Design Principles. Harlow: Pearson Education Limited, 2018.