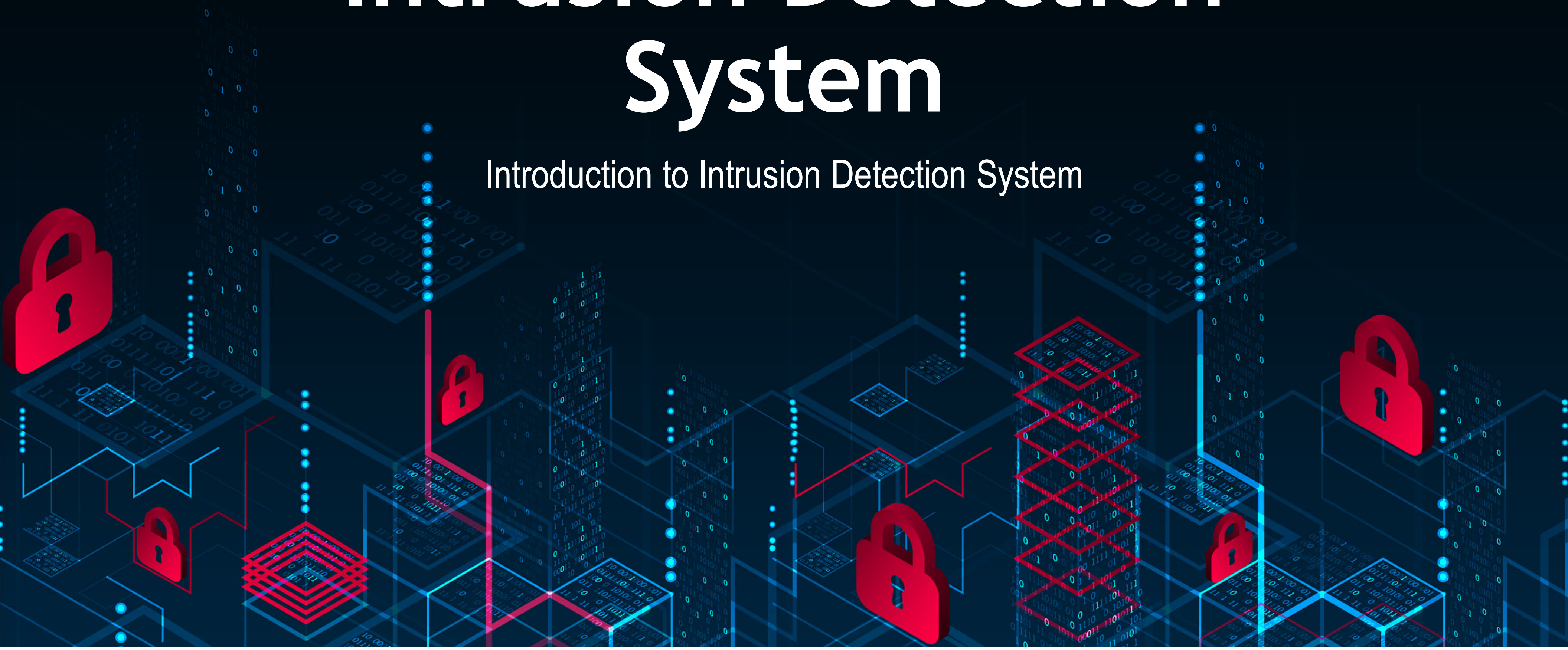
CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

Intrusion Detection System

Introduction to Intrusion Detection System



Video Summary

- What is Intrusion Detection System (IDS)
- Types of Intruders
- Intruder Skill Levels
- Examples of Intrusion
- IDS Requirements

Intrusion Detection

- **NIST SP 800-94**

Intrusion detection systems (IDSs) are software or hardware systems that automate the process of monitoring the events occurring in a computer system or network, analyzing them for signs of security problems.

Intruders and Intrusion Detection

- Successful attacks allow intruders to gain unauthorized access to resources
- Often cheaper to prevent some attacks and detect the rest
- Response from a detected attack may be technical or legal

Types of Intruders

- **Masquerader**

- Someone who is not authorized to use the system and penetrates access controls to exploit a legitimate user’s account “outsider”

- **Misfeasor**

- Legitimate user who accesses resources he is not authorized to, or misuse privileges “insider”

A student who has a canvas account can escalate the privileges to be able to modify the grades

- **Clandestine user**

- Takes administrator control of a system and uses it to avoid detection “insider or outsider”

Intruder Skill Levels - Apprentice

- Hackers with minimal technical skill who primarily use existing attack toolkits
- They likely comprise the largest number of attackers, including many criminal and activist attackers
- Given their use of existing known tools, these attackers are the easiest to defend against
- Also known as “script-kiddies” due to their use of existing scripts (tools)

Intruder Skill Levels - Journeyman

- Hackers with sufficient technical skills to modify and extend attack toolkits to use newly discovered, or purchased, vulnerabilities
- They may be able to locate new vulnerabilities to exploit that are similar to some already known
- Hackers with such skills are likely found in all intruder classes
- Adapt tools for use by others

Intruder Skill Levels - Master

- Hackers with high-level technical skills capable of discovering brand new categories of vulnerabilities

- Write new powerful attack toolkits

- Some of the better known classical hackers are of this level

- Some are employed by state/government-sponsored organizations

- Defending against these attacks is of the highest difficulty

Examples of Intrusion

- **Remote root/administrator access**
- Aim is to compromise the service
- **Defacing a web server**
- Put something on the website so that the organization looks bad
- **Guessing/obtaining passwords**
- Internal users can try to get the database of passwords
- **Copying databases containing private information**
- Credit card numbers

Examples of Intrusion

- **Viewing sensitive data**
- Payroll records, medical information, financial information
- **Capturing network packets**
- Obtaining usernames and passwords
- **Using computer resources to distribute illegal material**
- Accessing another computer then initialize a DDoS attack
- **Using unattended, logged-in computer without permission**
- Forgot to log out on a public computer

Intruder Behavior

- **Cracker/hacker**

- Someone is trying to gain access to the system to intrude
- Motivated by thrill of access and/or status
- Look for easy targets; may share information with others (sharing groups)
- Use security flaws/bugs in software to gain access

- **Criminal Enterprise**

- Motivated by financial reward and/or political/religious ideologies
- Corporations, government funded
- Specific targets
- Avoid publicity (they are not looking for recognition or status)
- Use security flaws and social engineering to gain access

Intruder Behavior

➢ **Internal Threat**

- Motivated by revenge and/or entitlement
- Have access to system
- Difficult to detect
- Internal security mechanisms are useful:
    - least privilege,
    - strong authentication,
    - log and auditing,
    - employee termination policies (xEmployee)

Intrusion Techniques

- **Aim:** Gain access to system or increase privileges on system

- **Exploit flaws in software**

  - Bugs in software that allow execution of code by intruder
  - Solution: keep track of vulnerabilities + regular software updates and being up-to-date with alerts related to your system software https://www.securityfocus.com/

- **Acquire protected information**

  - Passwords guessing or cracking
  - Social engineering attacks
  - Solution: appropriate technologies, policies and education for confidential information

IDS Requirements

- Run continually with minimal human supervision
- Recover from system restart/crashes
- Monitor itself and detect attacks on itself
- Impose minimal overhead on system
- Configurable according to system security policies
- Adapt to system and user behaviour changes over time
- Scale to monitor large number of hosts
- Still (partially) work if some components stop working

Video Summary

- What is Intrusion Detection System (IDS)
- Types of Intruders
- Intruder Skill Levels
- Examples of Intrusion
- IDS Requirements