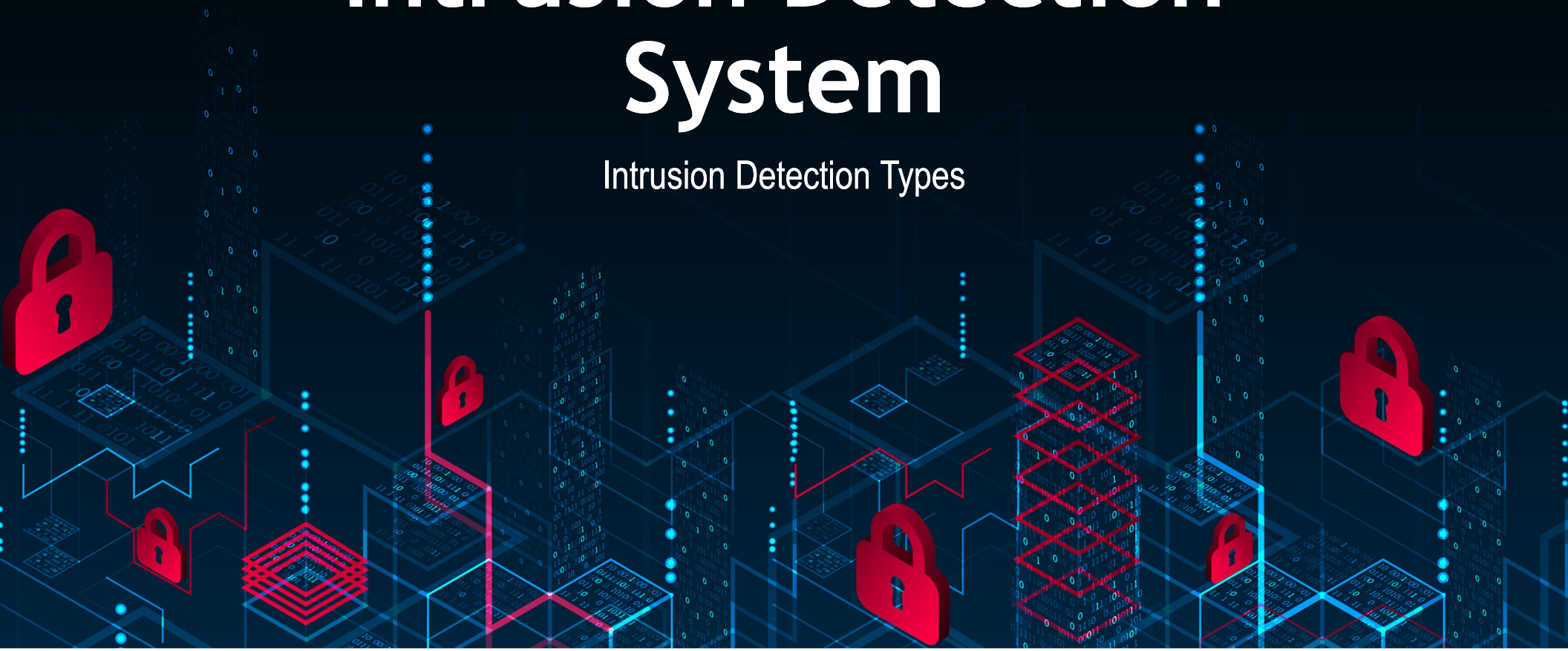
CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

Intrusion Detection System

Intrusion Detection Types



Video Summary

- IDS Components and Principles
- Example Measures for Intrusion Detection
- Example of Suspicious Activities
- Intrusion Detection Types

Intrusion Detection - Common Components

- **Sensor**
  - Collect data (tcpdumb), e.g. packets, log files, system call traces
- **Analyzers**
  - Receive collected data, analyze it and determine if intrusion
- **User Interface**
  - Allow user to view output and control behavior of IDS

Intrusion Detection System - Principles

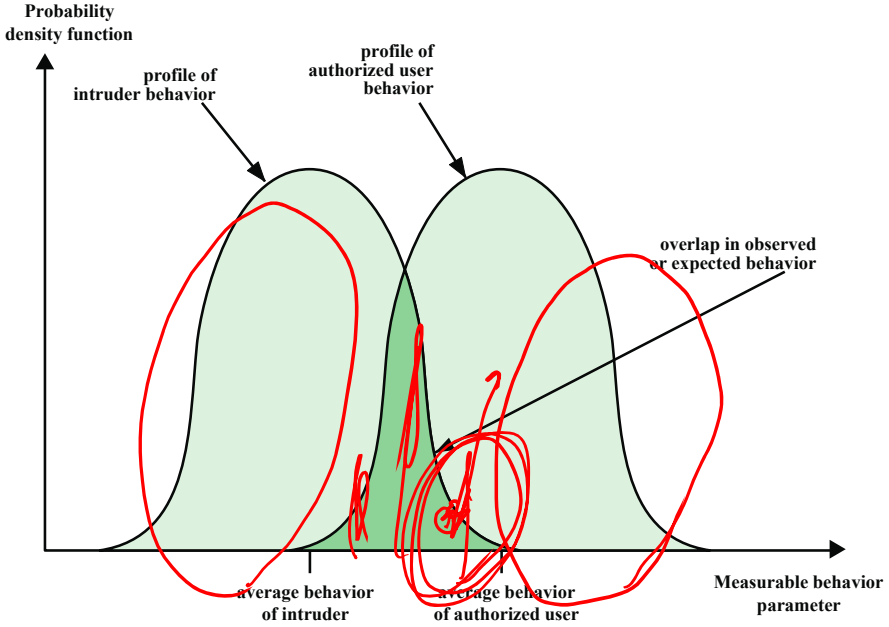


Figure 8.1 Profiles of Behavior of Intruders and Authorized Users

False positives: legitimate user identified as intruder
False negatives: intruder identified as a legitimate user

Example Measures for Intrusion Detection

Login and Session Activity	
Measure	Type of Intrusion Detected
Login frequency by day and time	Intruders may be likely to log in during off hours
Frequency of login at different locations	Intruders may log in from a location that a particular user never uses
Time since last login	Break-in on a "dead" account
Elapsed time per sessions	Significant deviations might indicate masquerader
Quantity of output to location	Excessive amounts of data transmitted to remote locations could signify leakage of sensitive data
Session resource utilisation	Unusual processor or I/O levels could signal intruder
Password failures at login	Attempted break-in by password guessing
Failures to login from specified terminals	Attempted break-in

Example Measures for Intrusion Detection

Command or Program Execution Activity

Execution frequency	Detect intruders based on their use of different commands
Program resource utilisation	Increased processor utilisation or I/O may indicate virus/Trojan
Execution denials	May detect attempt by user seeking higher privileges

File Access Activity

Read, write, create, delete frequency	Abnormal values may indicate masquerading
Records read, written	Abnormal values may indicate attempt to obtain sensitive data
Failure count for read, write create, delete	May detect users who persistently attempt to access unauthorised files

Example of Suspicious Activities

Excessive network traffic	Increased % utilization
Network traffic not normally present on the network	Multiple incorrect login attempts
Unusual data sharing between apps	Network and port scans
Unauthorized packet capturing	Unexpected file modifications

Intrusion Detection Types

- **Host-based IDS**
  - Monitor characteristics of a single computer
- **Distributed host-based IDS**
  - Monitor characteristics on set of computers with central module detecting intrusions
- **Network-based IDS**
  - Monitor network traffic to identify suspicious activities

Host-Based IDS

- Special layer of software to protect vulnerable systems
- It is very effective at identifying insider abuse
- Primary purpose: detect intrusions, log suspicious events, send alerts
- May be able to stop attacks if detected early
- Can detect both internal and external attacks
- Can use anomaly detection and/or signature detection

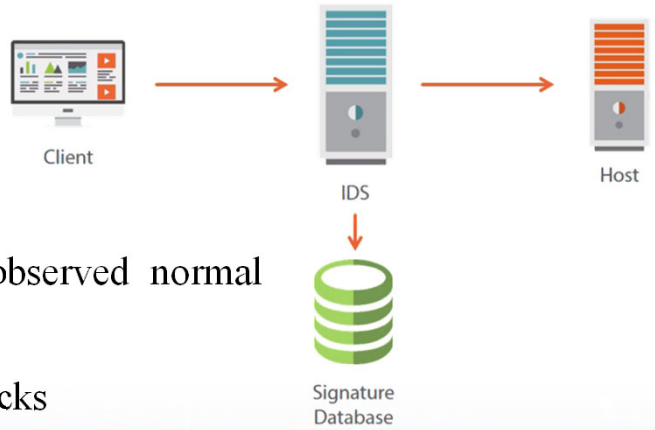
Anomaly vs Signature Detection

➢ **Anomaly Detection**

- Compare observed behavior against previously collected normal behavior
- Threshold detection: thresholds based on frequency of occurrence of events, independent of user
- Profile-based: profiles of users created and compared against

➢ **Signature Detection**

- Define attacks by set of rules or patterns
- Rule-based anomaly detection: define rules based on past observed normal behavior
- Rule-based penetration identification: define rules based on attacks



Anomaly Detection

A variety of classification approaches are used:

Statistical	Knowledge based	Machine-learning
• Monitor network traffic and compare it against an established basline (regular daily traffic)	• Approaches use an expert system that classifies observed behavior according to a set of rules that model legitimate behavior	• Approaches automatically determine a suitable classification model from the training data using data mining techniques

Signature or Heuristic Detection

Signature approaches

Match a large collection of known patterns of malicious data against data stored on a system or in transit over a network

The signatures need to be large enough to minimize the false alarm rate, while still detecting a sufficiently large fraction of malicious data

Widely used in anti-virus products, network traffic scanning proxies, and in NIDS

Rule-based heuristic identification

Involves the use of rules for identifying known penetrations or penetrations that would exploit known weaknesses

Rules can also be defined that identify suspicious behavior, even when the behavior is within the bounds of established patterns of usage

Typically rules used are specific

SNORT is an example of a rule-based NIDS

Audit Records

- **Native**
  - Most operating systems have logs of software and user activities
  - Advantage: no additional collection software needed
  - Disadvantage: information may not contain all needed information or in inconvenient form
  - Example: Windows event log
- **Detection-specific**
  - Records generated specifically for IDS
  - Advantages: may work on different systems
  - Disadvantage: extra overhead in collecting information
  - Example: Linux /var/log

Audit Records

Linux /var/log

```
alternatives.log          denyhosts.5.gz   mail.info.3.gz
alternatives.log.1        denyhosts.6.gz   mail.info.4.gz
alternatives.log.10.gz    denyhosts.7.gz   mail.log
alternatives.log.11.gz    dmesg            mail.log.1
alternatives.log.12.gz    dmesg.0          mail.log.2.gz
alternatives.log.2.gz     dmesg.1.gz       mail.log.3.gz
alternatives.log.3.gz     dmesg.2.gz       mail.log.4.gz
alternatives.log.4.gz     dmesg.3.gz       mailman
alternatives.log.5.gz     dmesg.4.gz       mail.warn
alternatives.log.6.gz     dpkg.log         mail.warn.1
alternatives.log.7.gz     dpkg.log.1       mail.warn.2.gz
alternatives.log.8.gz     dpkg.log.10.gz   mail.warn.3.gz
alternatives.log.9.gz     dpkg.log.11.gz   mail.warn.4.gz
apache2                   dpkg.log.12.gz   messages
apt                       dpkg.log.2.gz    messages.1
aptitude                  dpkg.log.3.gz    messages.2.gz
aptitude.1.gz             dpkg.log.4.gz    messages.3.gz
aptitude.2.gz             dpkg.log.5.gz    messages.4.gz
auth.log                  dpkg.log.6.gz    mysql
auth.log.1                dpkg.log.7.gz    mysql.err
```

Audit Records

Invalid password

```
auth.log:Jan 26 09:30:12 ict sshd[23778]: Failed password for root from 124.219.196.188 port 37684 ssh
2
auth.log:Jan 26 09:30:15 ict sshd[23780]: Failed password for root from 124.219.196.188 port 40043 ssh
2
auth.log:Jan 26 09:30:18 ict sshd[23782]: Failed password for root from 124.219.196.188 port 42285 ssh
2
auth.log:Jan 26 09:30:21 ict sshd[23784]: Failed password for root from 124.219.196.188 port 44641 ssh
2
auth.log:Jan 26 09:30:25 ict sshd[23786]: Failed password for root from 124.219.196.188 port 46722 ssh
2
auth.log:Jan 26 09:30:28 ict sshd[23788]: Failed password for root from 124.219.196.188 port 49076 ssh
2
```

```
auth.log:Jan 26 16:22:30 ict sshd[30606]: Failed password for root from 119.10.114.52 port 61996 ssh2
auth.log:Jan 26 16:22:35 ict sshd[30608]: Failed password for root from 119.10.114.52 port 64725 ssh2
auth.log:Jan 26 16:22:41 ict sshd[30610]: Failed password for root from 119.10.114.52 port 2521 ssh2
auth.log:Jan 26 16:22:47 ict sshd[30612]: Failed password for root from 119.10.114.52 port 4685 ssh2
auth.log:Jan 26 16:22:53 ict sshd[30614]: Failed password for root from 119.10.114.52 port 6724 ssh2
auth.log:Jan 26 16:27:22 ict sshd[30684]: Failed password for root from 61.174.51.209 port 3294 ssh2
auth.log:Jan 26 16:27:40 ict sshd[30686]: Failed password for root from 61.174.51.209 port 1284 ssh2
auth.log:Jan 26 16:28:00 ict sshd[30688]: Failed password for root from 61.174.51.209 port 4771 ssh2
auth.log:Jan 26 16:28:02 ict sshd[30688]: Failed password for root from 61.174.51.209 port 4771 ssh2
auth.log:Jan 26 16:28:19 ict sshd[30703]: Failed password for root from 61.174.51.209 port 2976 ssh2
auth.log:Jan 26 20:14:19 ict sshd[5991]: Failed password for root from 61.160.215.3 port 3419 ssh2
auth.log:Jan 26 20:14:39 ict sshd[5993]: Failed password for root from 61.160.215.3 port 3346 ssh2
```

Audit Records

Invalid user names

```
auth.log.4.gz:Jan  2 20:39:38 ict sshd[1821]: Failed password for invalid user a from 143.106.250.88 p
ort 49581 ssh2
auth.log.4.gz:Jan  3 02:42:40 ict sshd[7689]: Failed password for invalid user a from 124.115.18.12 po
rt 48478 ssh2
auth.log.4.gz:Jan  3 12:48:22 ict sshd[23878]: Failed password for u5422792754 from 203.131.209.66 por
t 56034 ssh2
auth.log.4.gz:Jan  3 16:50:11 ict sshd[28180]: Failed password for invalid user test from 222.219.187.
9 port 23713 ssh2
auth.log.4.gz:Jan  3 16:50:17 ict sshd[28182]: Failed password for invalid user test from 222.219.187.
9 port 25867 ssh2
auth.log.4.gz:Jan  3 16:50:30 ict sshd[28185]: Failed password for invalid user test from 222.219.187.
9 port 27524 ssh2
auth.log.4.gz:Jan  3 21:15:50 ict sshd[946]: Failed password for invalid user oracle from 113.108.211.
131 port 45802 ssh2
auth.log.4.gz:Jan  4 14:00:12 ict sshd[19921]: Failed password for invalid user zxin10 from 218.75.155
.14 port 37732 ssh2
auth.log.4.gz:Jan  4 14:00:18 ict sshd[19923]: Failed password for invalid user os10+ZTE from 218.75.1
55.14 port 38958 ssh2
auth.log.4.gz:Jan  4 14:00:23 ict sshd[19925]: Failed password for invalid user zxiptv from 218.75.155
.14 port 40226 ssh2
auth.log.4.gz:Jan  4 14:00:29 ict sshd[19927]: Failed password for invalid user zxin10 from 218.75.155
.14 port 41354 ssh2
auth.log.4.gz:Jan  4 14:00:34 ict sshd[19929]: Failed password for invalid user os10+ZTE from 218.75.1
55.14 port 42504 ssh2
auth.log.4.gz:Jan  4 14:00:40 ict sshd[19931]: Failed password for invalid user zxiptv from 218.75.155
.14 port 43674 ssh2
auth.log.4.gz:Jan  4 17:00:08 ict sshd[22704]: Failed password for invalid user auto from 89.248.172.5
8 port 49937 ssh2
auth.log.4.gz:Jan  4 17:00:12 ict sshd[22729]: Failed password for invalid user auto from 89.248.172.5
8 port 53354 ssh2
auth.log.4.gz:Jan  4 17:23:47 ict sshd[23098]: Failed password for invalid user ftpuser from 46.105.10
9.70 port 46965 ssh2
```

Video Summary

- IDS Components and Principles
- Example Measures for Intrusion Detection
- Example of Suspicious Activities
- Intrusion Detection Types