INTRUSION DETECTION SYSTEM (IDS)

by
Kilausuria Abdullah (GCIH)
Cyberspace Security Lab, MIMOS Berhad

OUTLINE

- Security incident
- Attack scenario
- Intrusion detection system
- Issues and challenges
- Conclusion

OUTLINE

- Security incident
- Attack scenario
- Intrusion detection system
- Issues and challenges
- Conclusion

Security incident landscape in Malaysia

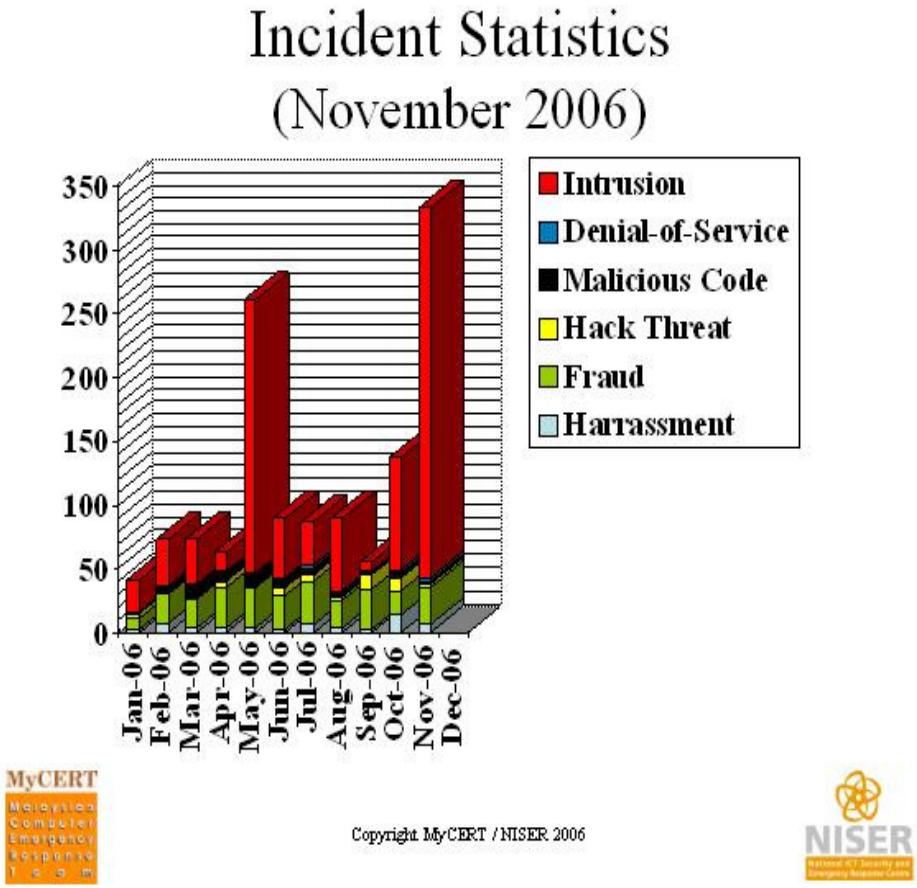


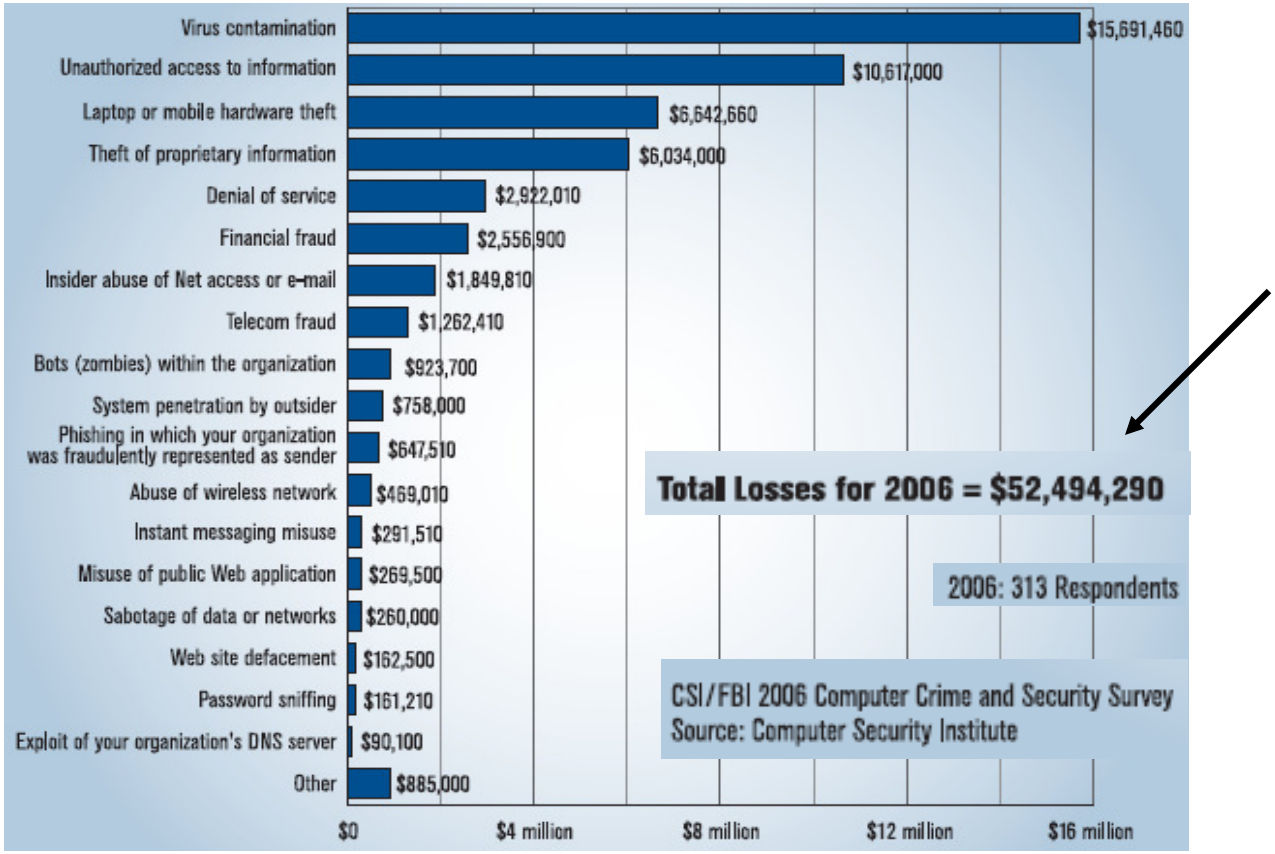
Fig 1: Mycert quarterly report

-High value that contributed to intrusion

-Total intrusion reported that related to intrusion (excluding spam) is more than 300 cases

Losses incurred from security incident

- Total losses have also declined, could be related to reduced in number of incidents reported

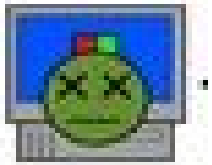


Source: CSI, CSO, PWC, MIMOS Analysis,

Pre-attack

Victim

Attacker



Target

Post-attack

Security incidents from intruder view

- an attack is unsuccessful from the perspective of intruder if none of their objective are fulfilled
- some components of an attack from the perspective an intruder are :
  - Objective ?
  - Exploits scripts ?
  - Vulnerabilities in target system ?
  - Risk carrying out an intrusion ?
  - Damage caused or consequences to victim ?

intruder

Security Incident from victim view

• A victim perspectives on intrusion is an attack is unsuccessful if there are no consequences that result from the attack

• Some components of an attack from the perspective of a victim are :

-What happened ?

-Who is affected ?

-Who is the intruder ?

-How did the intrusion happen ?

victim

OUTLINE

- Security incident
- Attack scenario
- Introduction to IDS
- IDS technologies
- Issues and challenges
- Conclusion

Attack scenario

- There are 5 steps involved in the attack scenario :

1. Reconnaissance
2. Scanning
3. Exploit the system
4. Keeping access
5. Covering the track

- Basically analyst use this flow of attack scenario to detect an attack. Intruder may not use all the 5 steps, it depends on the modus operandi and skills of the intruder.

Step 1 : Reconnaissance

- Conduct open source investigation to extract information about a target such as domain name server (DNS), internet protocol (IP) and staff information

Reconnaissance tool	Description
Whois	Acquire name servers
DNS interrogation	Domain name and IP address
Web site searchers	Acquiring information about company from public databases
Google	Googling for vulnerable system and etc
Sam Spade	Capabilities such : ping, DNS lookup, whois, DNS zone transfer, trace route, finger, check time
Web-based reconnaissance	Numerous web site offer the capability to research or attack other sites

Step 2 : Scanning

- An attacker uses a variety of vulnerability scanning tools to survey a target to find vulnerabilities in the target defenses

Scanning tool	Description
THC-scan	Scan network looking for unprotected modems that auto-answer with no passwords
War driving with NetStumbler	Trying to connect to unprotected wireless networks to gain network or internet access
Port Scanning with nmap	To see which port are open.
Vulnerability scanning nessus	Basically run port scanner and try to connect to each port

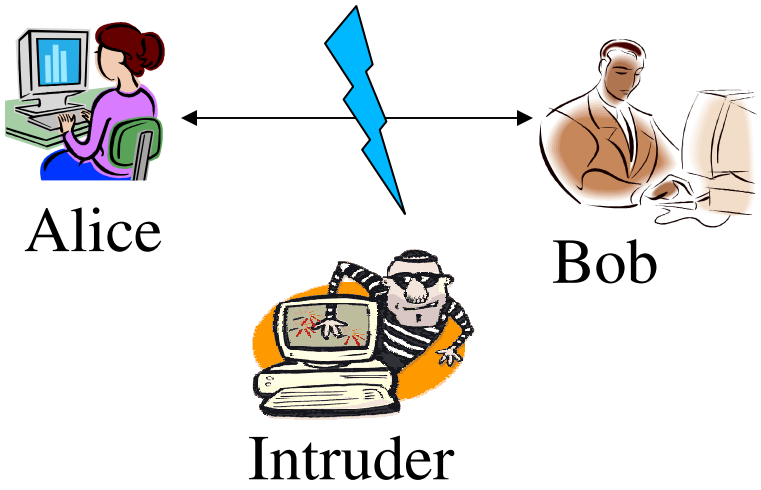
Step 3 : Exploit to system

- An attacker tries to gain access, undermine an application or deny access to other users
- There are 3 ways in exploit the system :
  - Gaining access
  - Web application attack
  - Denial of Service (DoS)

Gaining access

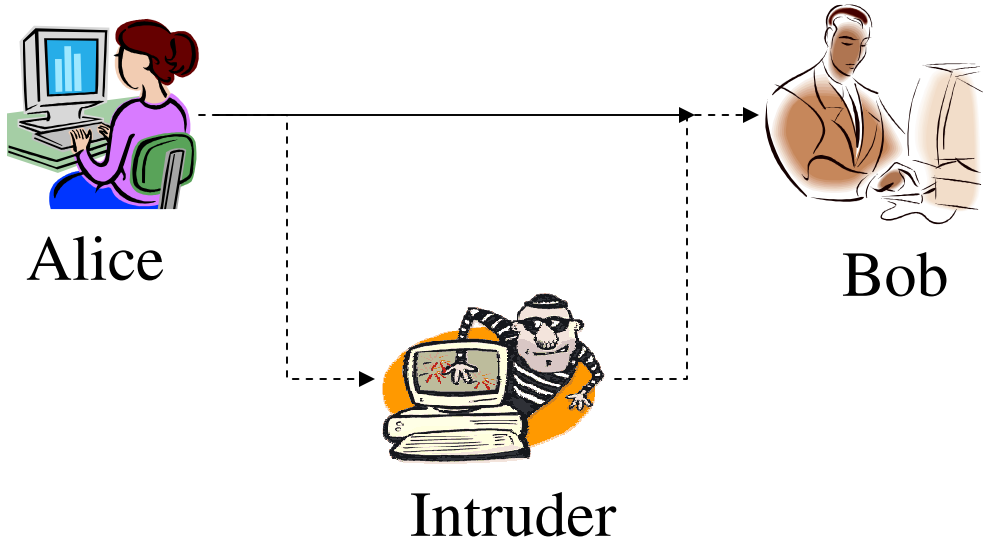
-Unauthorized access by eavesdropping into communication channel

-e.g : IP address spoofing, session hijacking, password cracking and worm



Step 3 : Exploit to system

Web Application attack



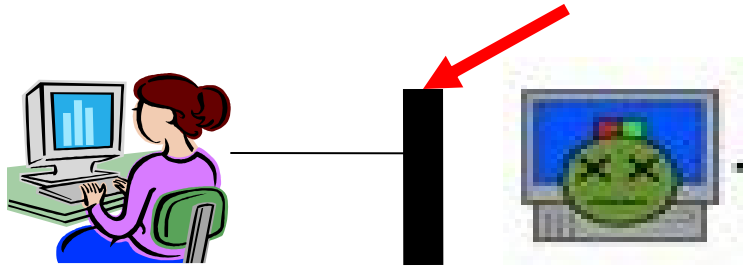
- The information not only intercepted, but modified by an unauthorized party while transit from the source to the destination

-example : account harvesting, SQL injection and cross-site scripting

ATTACK SCENARIO

Exploit to system

Denial of Service (DoS)

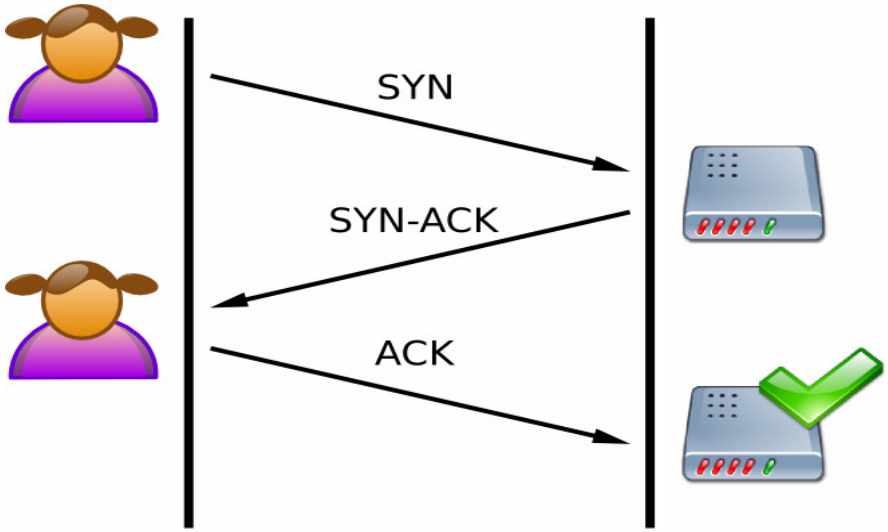


- An asset of the system gets destroyed or becomes unavailable

Launch	Local	Network-based
1.Stopping services	-process killing, -process crashing, -system reconfig	-spawning to fill process table -filling up the whole file system
2.Exhausting resources	- malformed packet(bonk)	- packet floods(SYN flood)

ATTACK EXAMPLE

SYN Flood Attack

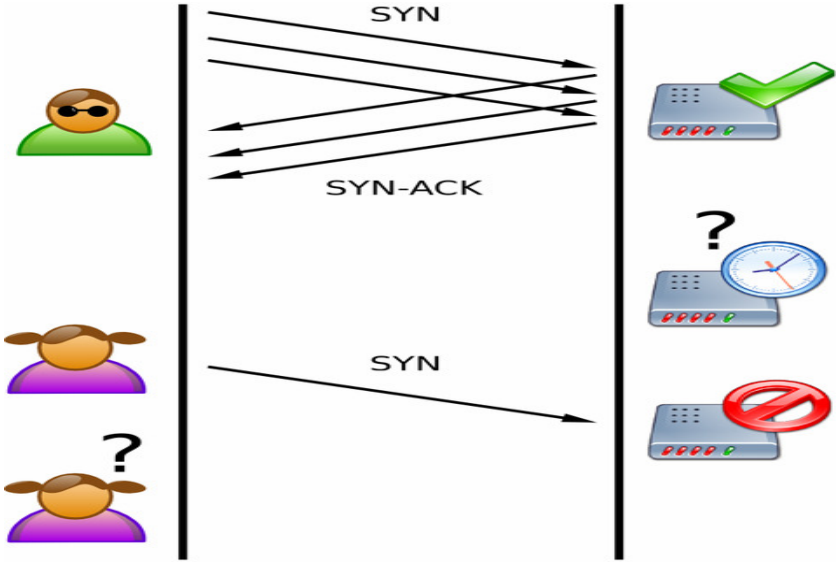


-A normal connection between a user (Alice) and a server.

-The three-way handshake is correctly performed.

ATTACK EXAMPLE

SYN Flood Attack



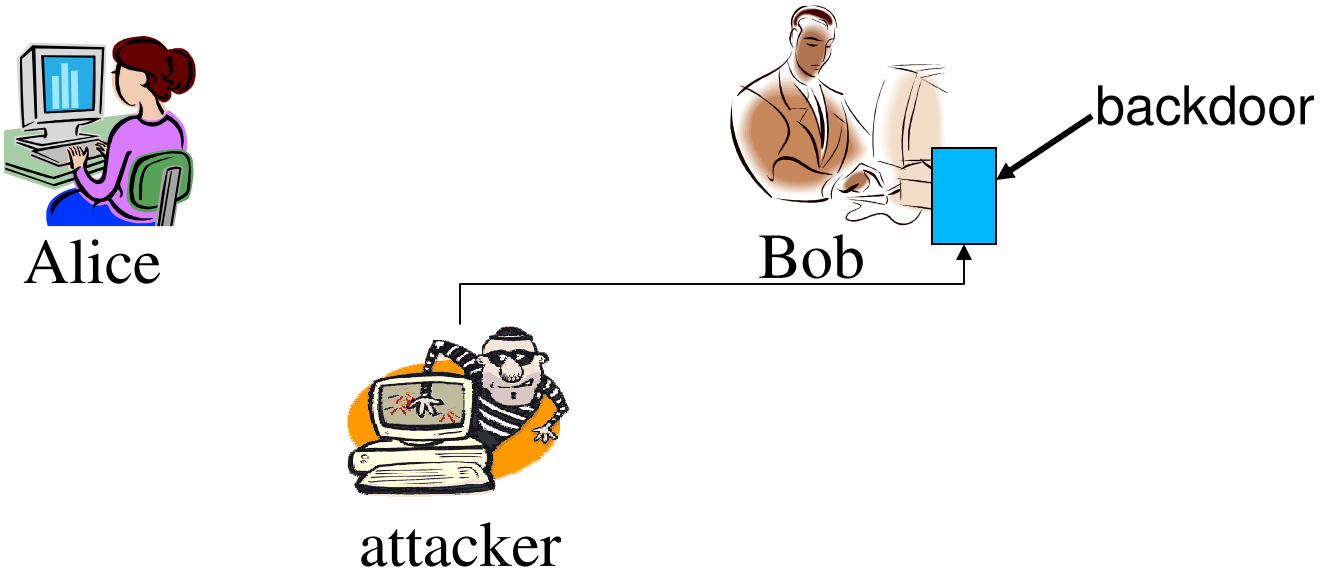
-The attacker (Bob) sends several packets but does not send the "ACK" back to the server.

-The connections are hence half-opened and eat the server resources.

-Alice, a legitimate user, tries to connect but the server refuses to open a connection resulting in a denial of service.

Step 4 : Keeping access

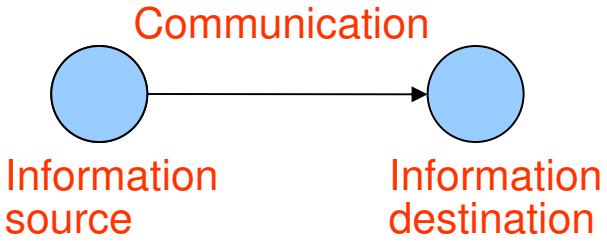
- Attacker maintain access by manipulating the software installed on the system to achieve backdoor access
- Example : backdoor and trojan horses

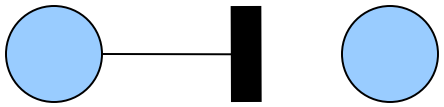


Step 5 : Covering the track

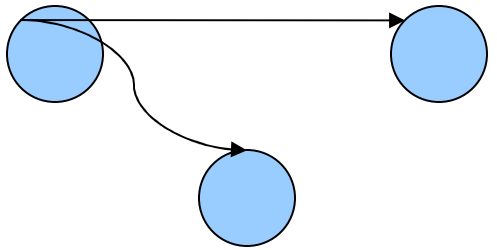
- Attacker maintain hard fought access by covering tracks. Hide from users and system admin using variety of techniques
- covering track in Unix, Windows and network is different
  - Hide files to simply name like dot space

Attack scenarios

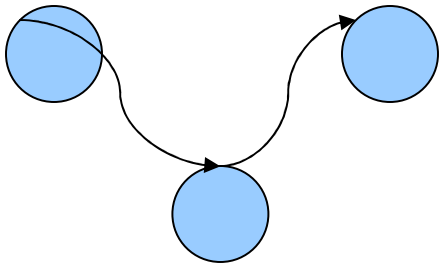




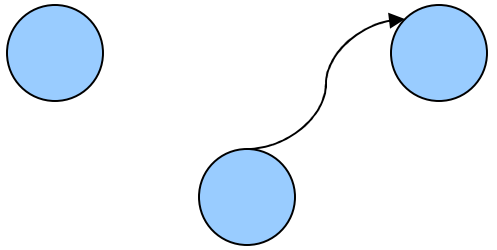
1. Interruption



2. Interception



3. Modification



4. Fabrication

OUTLINE

- Security incident
- Attack scenario
- Intrusion detection system
- Issues and challenges
- Conclusion

Intrusion detection system (IDS)

Intrusion:

Sequence related actions performed by a malicious adversary that results in the compromise of a target computing or networking domain

Intrusion detection :

Processes to identify and respond to malicious activity targeted at target computing and networking domain

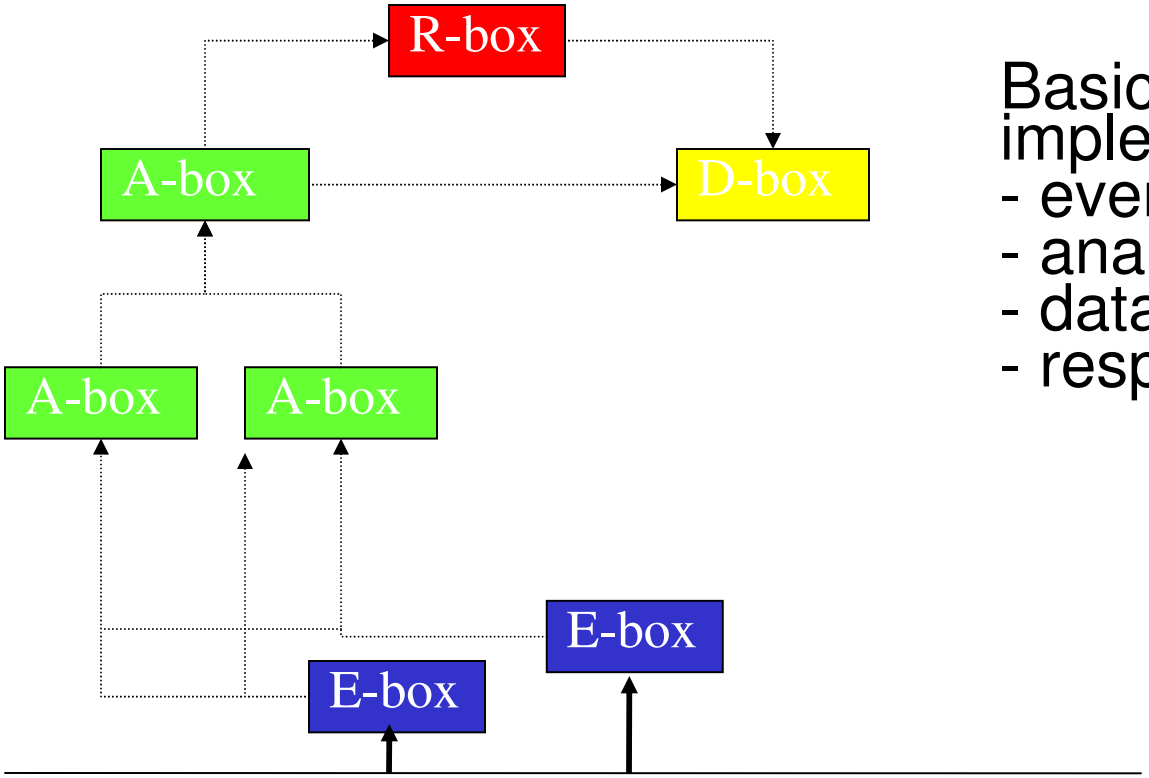
Intrusion Detection System (IDS):

is a system that automates the intrusion detection process

Terminology in IDS

- Attack
  - a failed attempt to enter the system
- False negative
  - test result implying a condition does not exist when in fact it does.
- False positive
  - test result implying a condition exists when in fact it does not.

Common Intrusion Detection Framework (CIDF), models an IDS aggregate as four component :



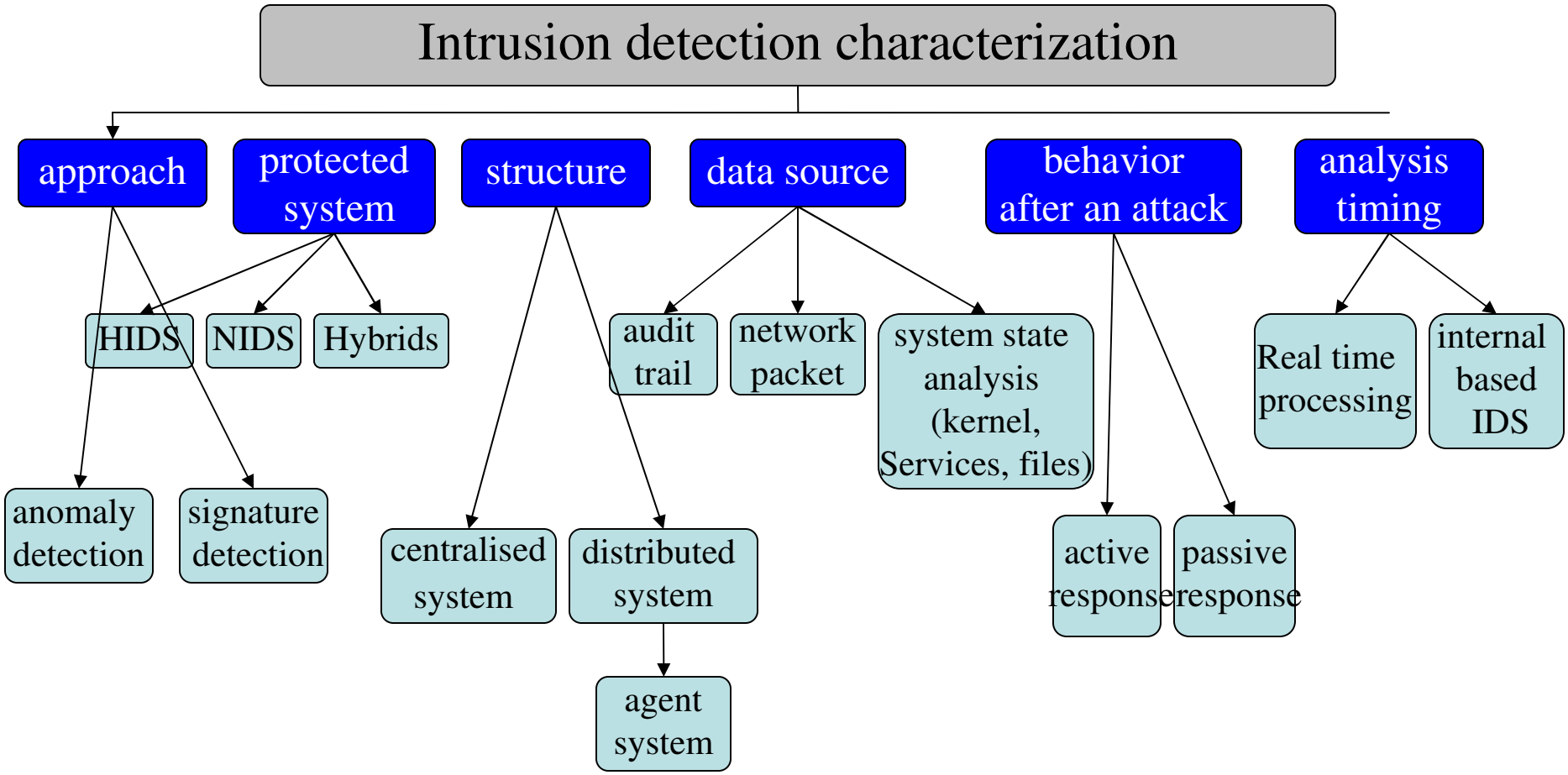
[Porras et al.,1998]

Basically in CIDF, IDS implementation have :
- event box (E-box)
- analysis box (A-box)
- database box (D-box)
- response box (R-box)

Exchange raw audit data

exchange events

Intrusion Detection Characterization

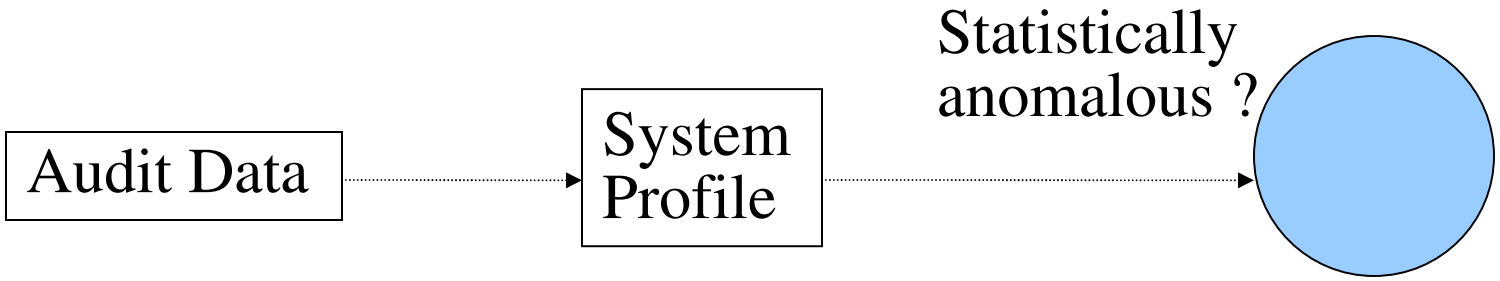


Source : przemyslaw & piotr

IDS approach

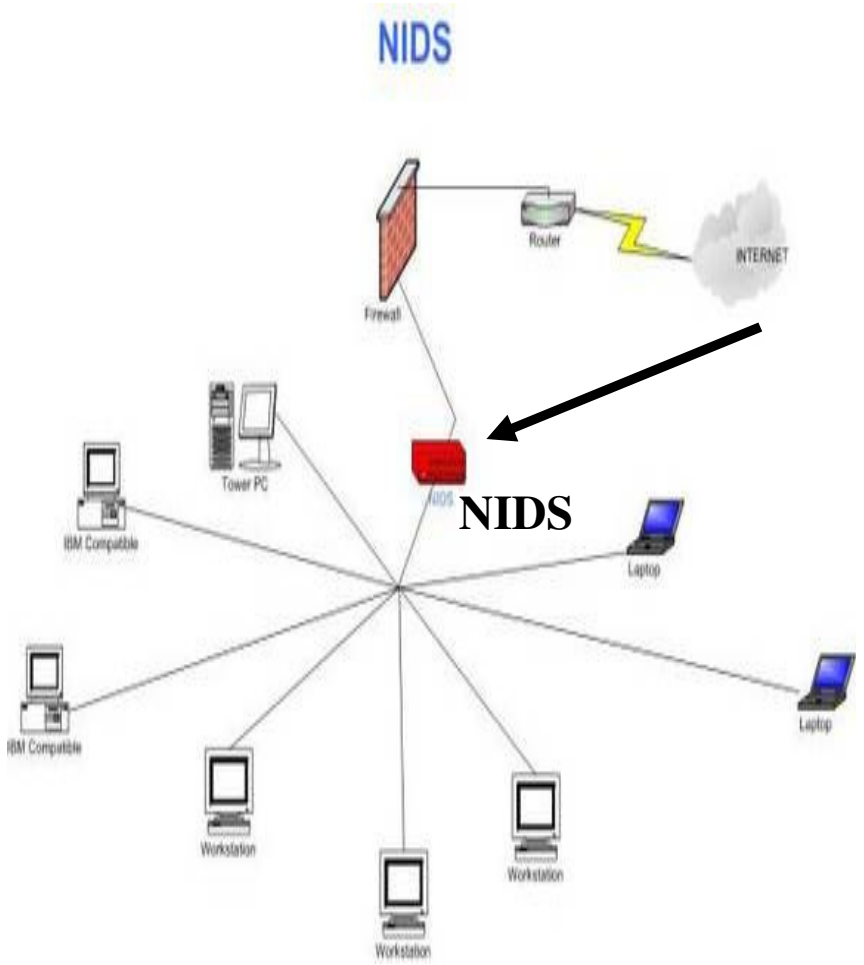
Signature vs Anomaly

1.Signature based – Audit data collected by the IDS is compared with the content of the signature, if a match IS found, alert generated



2.Anomaly based – Audit data collected by the IDS is compared with the system profile (normal behaviour), if a match NOT found, alert generated

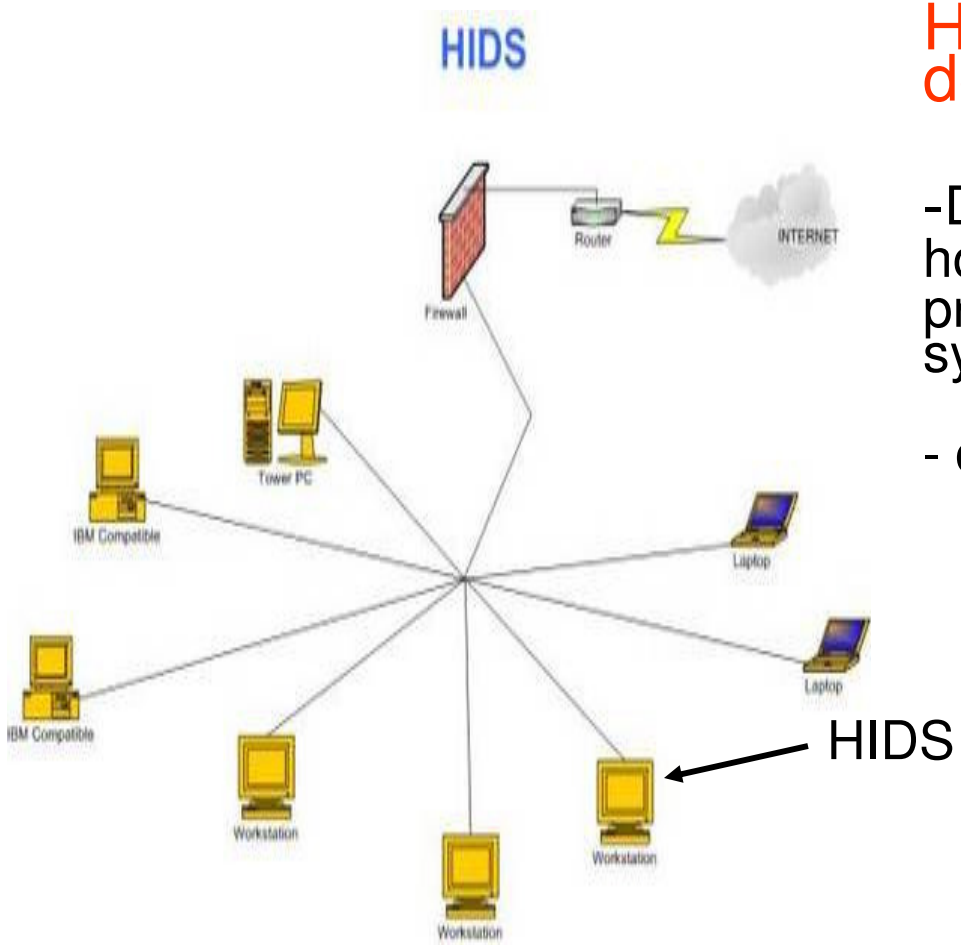
Protected system in IDS



Network intrusion detection system (NIDS)

- Detects attack by analyzing the network traffic exchanged on a network link .

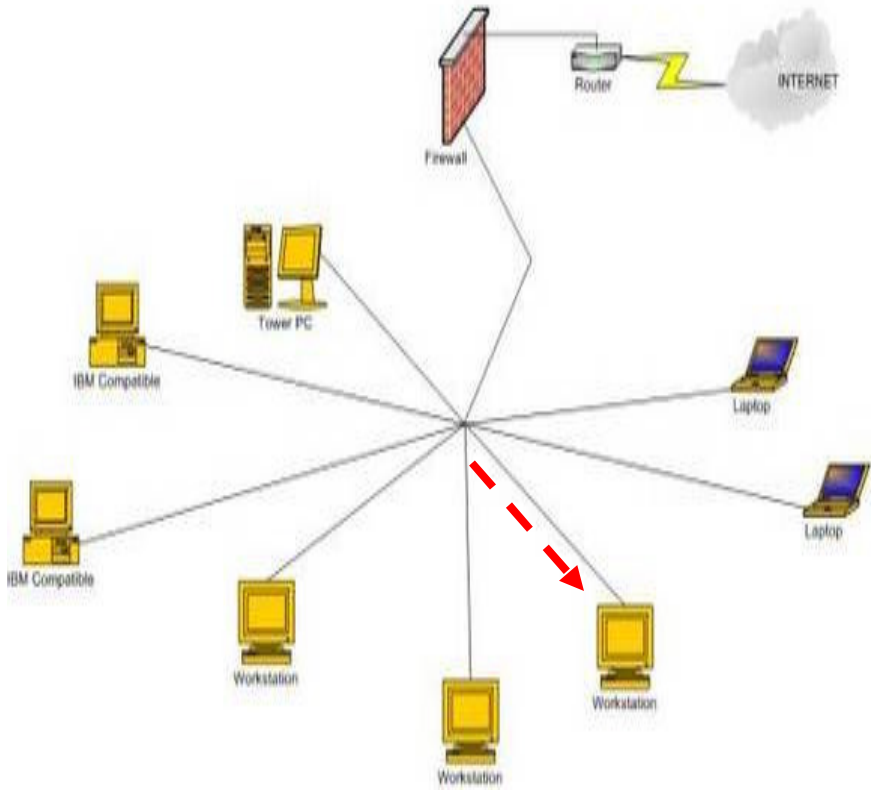
- defense at the network level



Host-based intrusion detection system(HIDS)

-Detects attack against a specific host by analyzing audit data produced by the host operating system

- defense at the application level



Hybrids

- Detects attack against a specific host by analyzing audit data produced by the host operating system and network traffic

IDS structure

Centralized system
- IDS can operate standalone

Centralized application
- integrated applications that create a distributed system
- multiple IDS

Agent
- a particular architecture with autonomous agents that are able to take pre-emptive and reactive measures and even to move over the network

IDS Data Source

- Audit trail – event log processing
- Network packet – a stream of network packet
- System state analysis -from kernel, services, files

IDS Behaviour after attack

- Active Response
  - IDS responds to the suspicious activity by logging off a user or by reprogramming the firewall to block network traffic from the suspected malicious source.

- Passive Response
  - IDS detects a potential security breach, logs the information and signals an alert

IDS Analysis Timing

- Real time processing
  - Perform online verification of system events
  - Require large amount RAM since no data storage is used
  - Online monitoring, analyze events and user actions

- Interval based
  - Related to audit trail (event log processing)
  - Recording every event, consumption of system resources
  - Vulnerable to DoS attack by over flowing the system's free space

IDS Technologies

- IDS product
  - Non commercial IDS
    - Snort, Emerald, Netstat, Bro and many others
  - Commercial IDS
    - SourceFire, NetProwler, NetRanger, Centrax, RealSecure and many others

IDS TECHNOLOGIES

- Immature and dynamic
- Research product
  - eg. Emerald, Netstat, Bro etc
- Commercial products (CMDS, NetProwler, NetRanger, Centrax, RealSecure etc

OUTLINE

- Security incident
- Attack scenario
- Intrusion detection system
- Issues and challenges
- Conclusion

IDS issues and challenges

- Operational challenges with IDS
  - Too many of IDS product
    - IDS do not have the capability to look at every possible security event
  - Difficulty with evaluating IDS technologies
    - Identify and evaluate the processes,procedures and tools
  - Lack of qualified technical staff
    - To evaluate, select, install, operate and maintain IDS technologies
- Events from multiple sources
  - Need to correlate the event

IDS issues and challenges

- IDS vs Intrusion prevention system (IPS)

  - IPS is a system to detect and also prevent the intrusion

  - The difference between IPS and IDS mainly it has the prevention process in line

- Will IPS replace IDS?
  - Use both

Conclusion

- IDS is a technology that can be use to detect an attack , but for future capabilities in IDS can be improved

References :

Christopher Kruegel, Fredrik Valeur, Giovanni Vigna (2005). Intrusion Detection and Correlation, Challenges and Solution, Springer Science+Business Media Inc, USA.

Ed Skoudis and SANS. Computer and network hacking exploits –SANS 2006

http://www.sei.cmu.edu/publications/documents/99.reports/99tr028/99tr028chap01.html

http://www.windowsecurity.com/articles/IDS-Part2-Classification-methods-techniques.html

MIMOS

Innovation for Life

Thank you