Intrusion Detection System

Click to add Text

cuu duong than cong . com

Most Slides are From Computer Security: Principles and Practice

Chapter 6 – Intrusion Detection

Click to add Text

First Edition

by William Stallings and Lawrie Brown

Lecture slides by Lawrie Brown

Intruders

- significant issue hostile/unwanted trespass
  - from benign to serious
- user trespass
  - unauthorized logon, privilege abuse
- software trespass
  - virus, worm, or trojan horse
- classes of intruders:
  - masquerader, misfeasor, clandestine user

Examples of Intrusion

- remote root compromise
- web server defacement
- guessing / cracking passwords
- copying viewing sensitive data / databases
- running a packet sniffer
- distributing pirated software
- using an unsecured modem to access net
- impersonating a user to reset password
- using an unattended workstation

Security Intrusion & Detection

Security Intrusion

a security event, or combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system (or system resource) without having authorization to do so.

Intrusion Detection

a security service that monitors and analyzes system events for the purpose of finding, and providing real-time or near real-time warning of attempts to access system resources in an unauthorized manner.

Intrusion Techniques

- objective to gain access or increase privileges
- initial attacks often exploit system or software vulnerabilities to execute code to get backdoor
  - e.g. buffer overflow
- or to gain protected information
  - e.g. password guessing or acquisition

cuu duong than cong . com

Hackers

- motivated by thrill of access and status
  - hacking community a strong meritocracy
  - status is determined by level of competence
- benign intruders might be tolerable
  - do consume resources and may slow performance
  - can't know in advance whether benign or malign
- IDS / IPS / VPNs can help counter
- awareness led to establishment of CERTs
  - collect / disseminate vulnerability info / responses

Hacker Behavior Example

1. select target using IP lookup tools
2. map network for accessible services
3. identify potentially vulnerable services
4. brute force (guess) passwords
5. install remote administration tool
6. wait for admin to log on and capture password
7. use password to access remainder of network

Criminal Enterprise

- organized groups of hackers now a threat
  - corporation / government / loosely affiliated gangs
  - typically young
  - often Eastern European or Russian hackers
  - common target credit cards on e-commerce server
- criminal hackers usually have specific targets
- once penetrated act quickly and get out
- IDS / IPS help but less effective
- sensitive data needs strong protection

Criminal Enterprise Behavior

1. act quickly and precisely to make their activities harder to detect
2. exploit perimeter via vulnerable ports
3. use trojan horses (hidden software) to leave back doors for re-entry
4. use sniffers to capture passwords
5. do not stick around until noticed
6. make few or no mistakes.

Insider Attacks

- among most difficult to detect and prevent
- employees have access & systems knowledge
- may be motivated by revenge / entitlement
  - when employment terminated
  - taking customer data when move to competitor
- IDS / IPS may help but also need:
  - least privilege, monitor logs, strong authentication, termination process to block access & mirror data

Insider Behavior Example

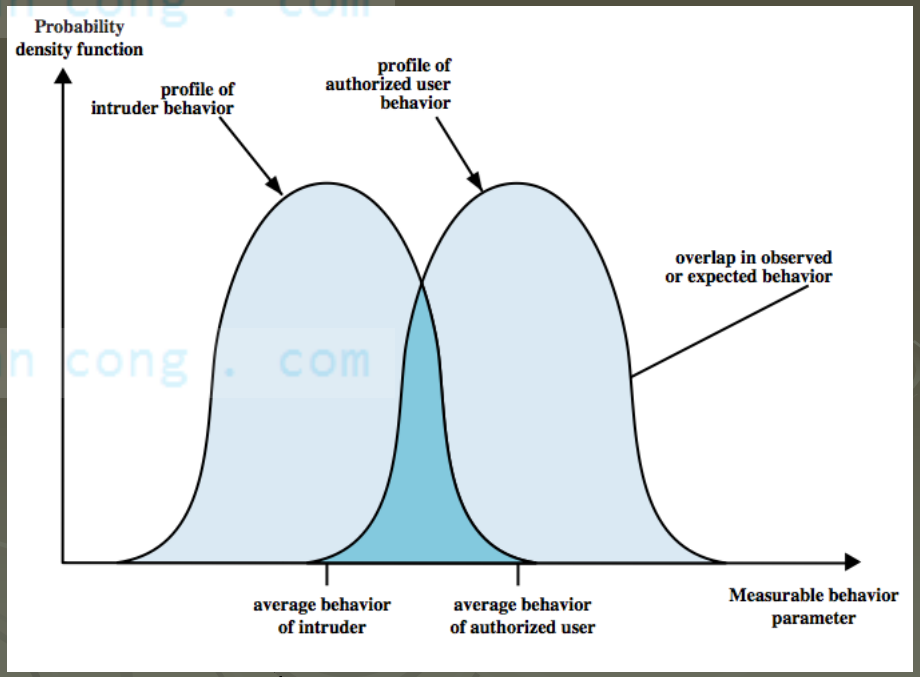
1. create network accounts for themselves and their friends
2. access accounts and applications they wouldn't normally use for their daily jobs
3. e-mail former and prospective employers
4. conduct furtive instant-messaging chats
5. visit web sites that cater to disgruntled employees, such as f'dcompany.com
6. perform large downloads and file copying
7. access the network during off hours.

Intrusion Detection Systems

- classify intrusion detection systems (IDSs) as:
  - Host-based IDS: monitor single host activity
  - Network-based IDS: monitor network traffic
- logical components:
  - sensors - collect data
  - analyzers - determine if intrusion has occurred
  - user interface - manage / direct / view IDS

IDS Principles

- assume intruder behavior differs from legitimate users
  - expect overlap as shown
  - observe deviations from past history
  - problems of:
    - false positives
    - false negatives
    - must compromise



IDS Requirements

- run continually
- be fault tolerant
- resist subversion
- impose a minimal overhead on system
- configured according to system security policies
- adapt to changes in systems and users
- scale to monitor large numbers of systems
- provide graceful degradation of service
- allow dynamic reconfiguration

Host-Based IDS

- specialized software to monitor system activity to detect suspicious behavior
  - primary purpose is to detect intrusions, log suspicious events, and send alerts
  - can detect both external and internal intrusions
- two approaches, often used in combination:
  - anomaly detection - defines normal/expected behavior
    - threshold detection
    - profile based
  - signature detection - defines proper behavior

Audit Records

- a fundamental tool for intrusion detection
- two variants:
  - native audit records - provided by O/S
    - always available but may not be optimum
  - detection-specific audit records - IDS specific
    - additional overhead but specific to IDS task
    - often log individual elementary actions
    - e.g. may contain fields for: subject, action, object, exception-condition, resource-usage, time-stamp

Example of Audit

- Consider copy.exe game.exe <system>/game.exe
- Several records may be generated for a single command
  1. Execute copy.exe
  2. Read game.exe
  3. Write <system>/game.exe

Anomaly Detection

- threshold detection
  - checks excessive event occurrences over time
  - alone a crude and ineffective intruder detector
  - must determine both thresholds and time intervals
- profile based
  - characterize past behavior of users / groups
  - then detect significant deviations
  - based on analysis of audit records
    - gather metrics: counter, guage, interval timer, resource utilization
    - analyze: mean and standard deviation, multivariate, markov process, time series, operational model

Examples of Anomaly

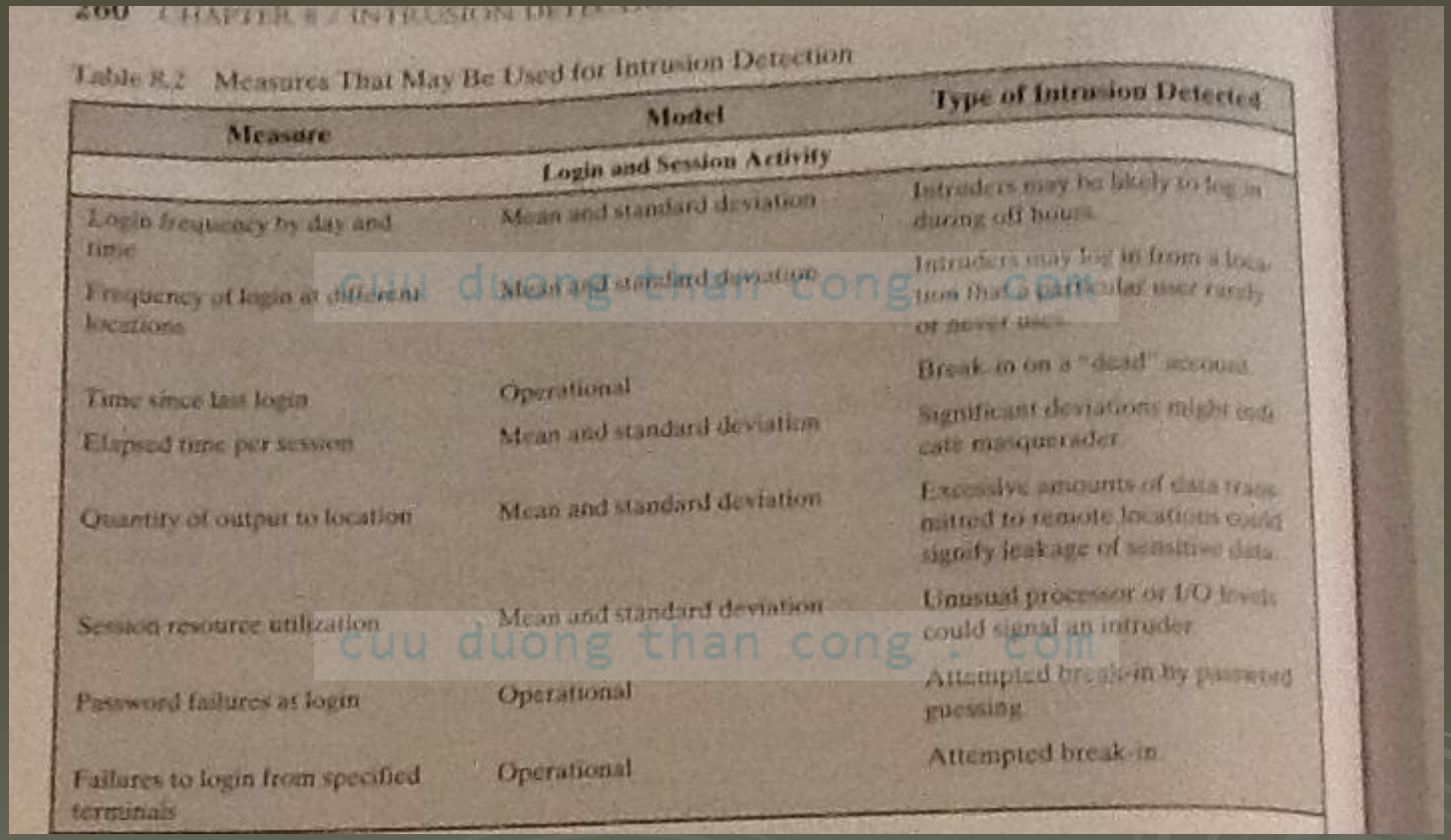


Table 8.2 Measures That May Be Used for Intrusion Detection

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

Examples of Anomaly

Command or Program Execution Activity		
Execution frequency	Mean and standard deviation	May detect intruders who are likely to use different commands, or a successful penetration by a legitimate user, who has gained access to privileged commands.
Program resource utilization	Mean and standard deviation	An abnormal value might suggest injection of a virus or Trojan horse, which performs side effects that increase I/O or processor utilization.
Execution denials	Operational model	May detect penetration attempt by individual user who seeks higher privileges.
Fil Access Activity		
Read, write, create, delete frequency	Mean and standard deviation	Abnormalities for read and write access for individual users may signify masquerading or browsing.
Records read, written	Mean and standard deviation	Abnormality could signify an attempt to obtain sensitive data by inference and aggregation.
Failure count for read, write, create, delete	Operational	May detect users who persistently attempt to access unauthorized files.

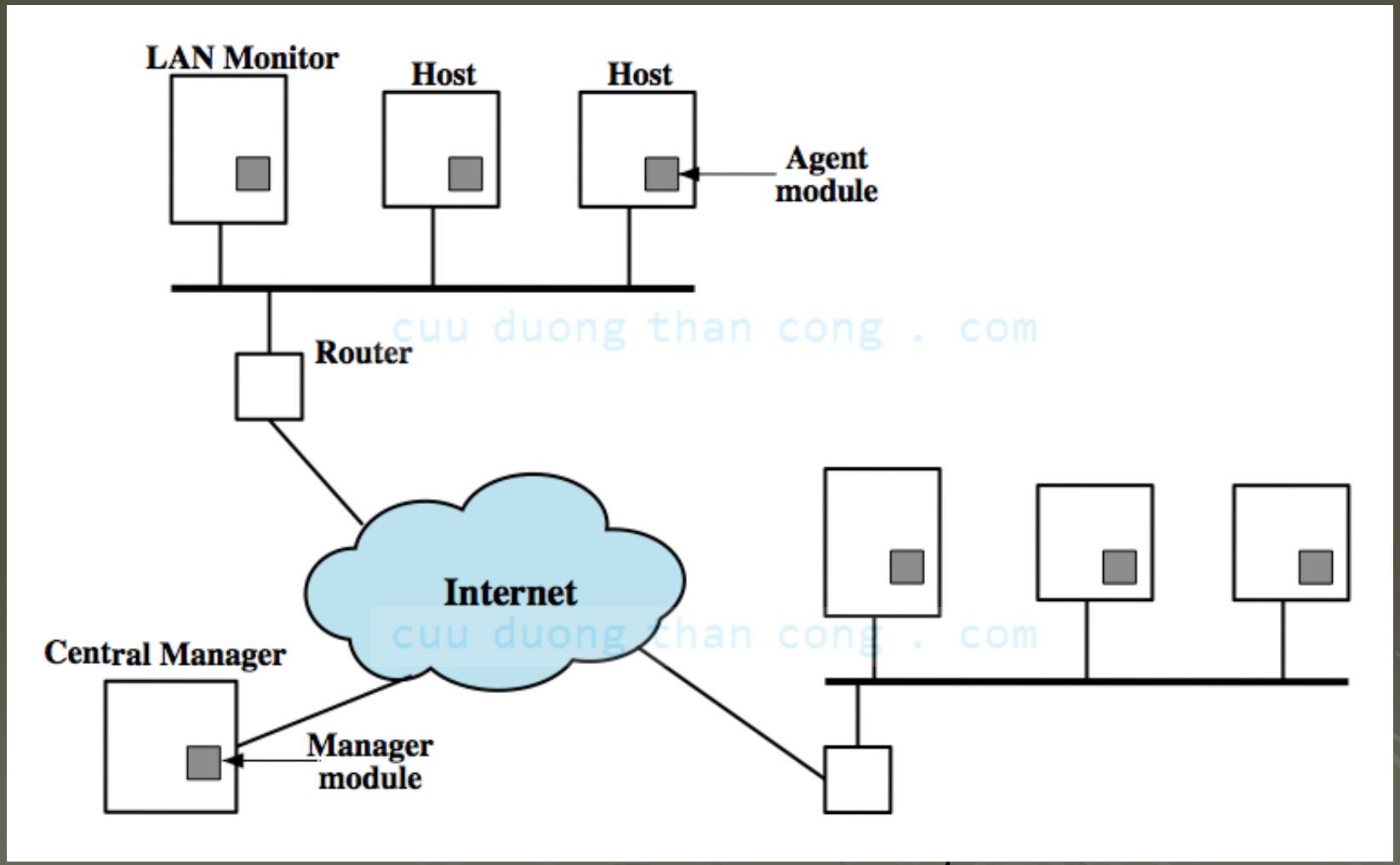
Signature Detection

- observe events on system and applying a set of rules to decide if intruder
- approaches:
  - rule-based anomaly detection
    - analyze historical audit records for expected behavior, then match with current behavior
  - rule-based penetration identification
    - rules identify known penetrations / weaknesses
    - often by analyzing attack scripts from Internet
    - supplemented with rules from security experts

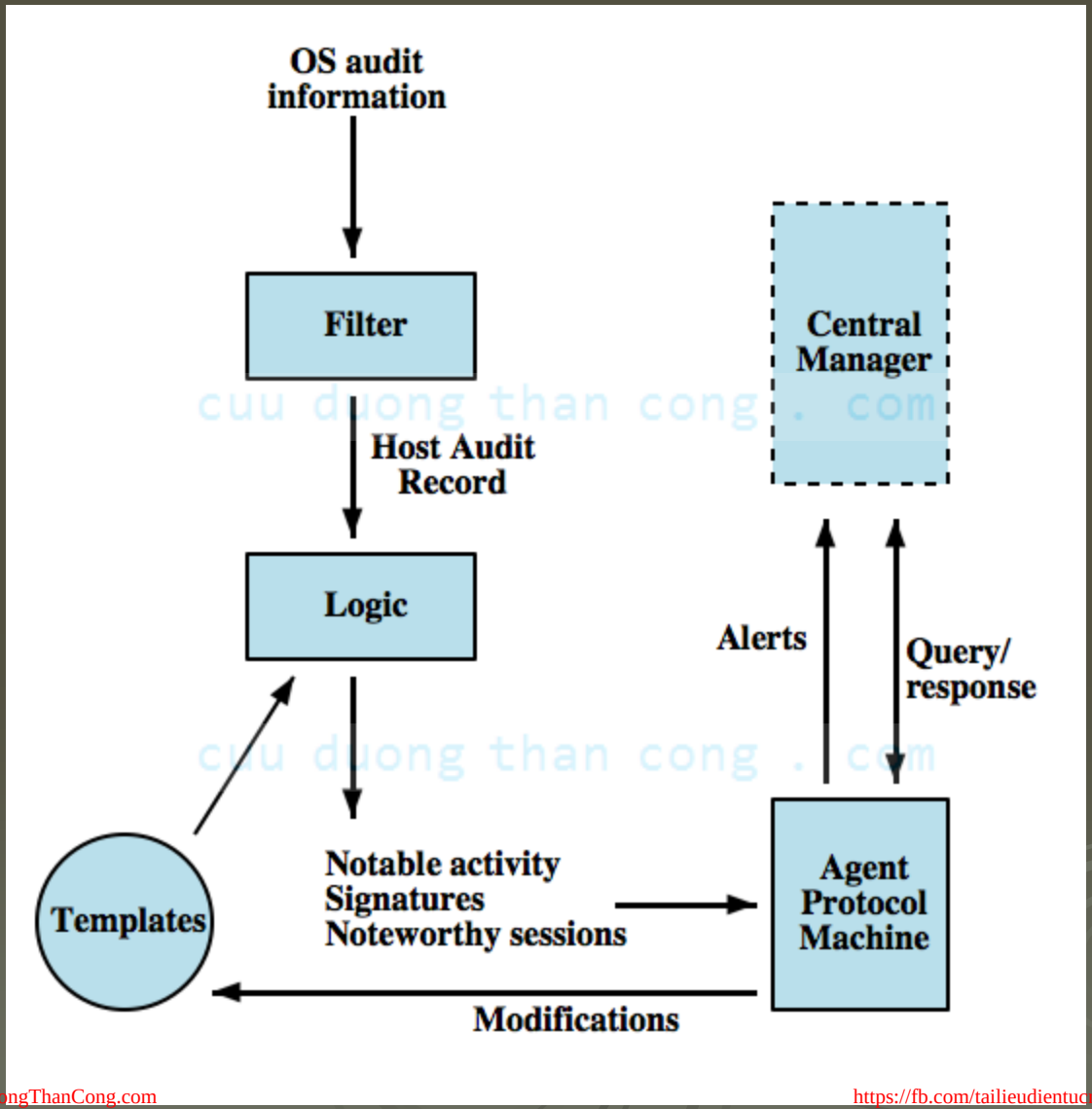
Example of Signatures

- Users should not read files in other users' personal directories
- Users must not write other users' files
- Users who log in after hours often access the same files they user earlier
- Users do not generally open disk devices but rely on higher-level operating system utilities
- Users should not be logged in more than once to the system
- Users do not make copies of system program

Distributed Host-Based IDS



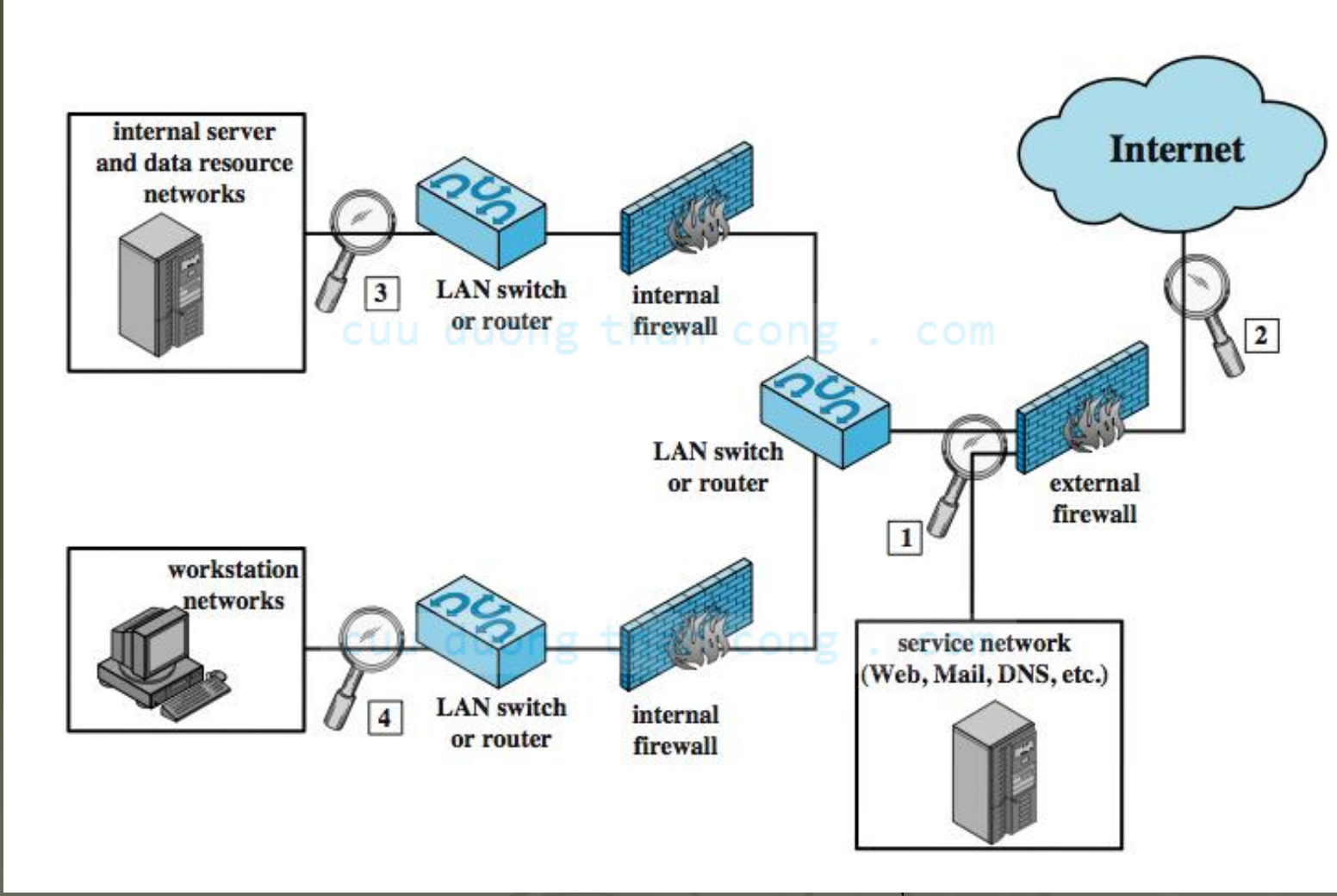
Distributed Host-Based IDS



Network-Based IDS

- network-based IDS (NIDS)
  - monitor traffic at selected points on a network
  - in (near) real time to detect intrusion patterns
  - may examine network, transport and/or application level protocol activity directed toward systems
- comprises a number of sensors
  - inline (possibly as part of other net device)
  - passive (monitors copy of traffic)

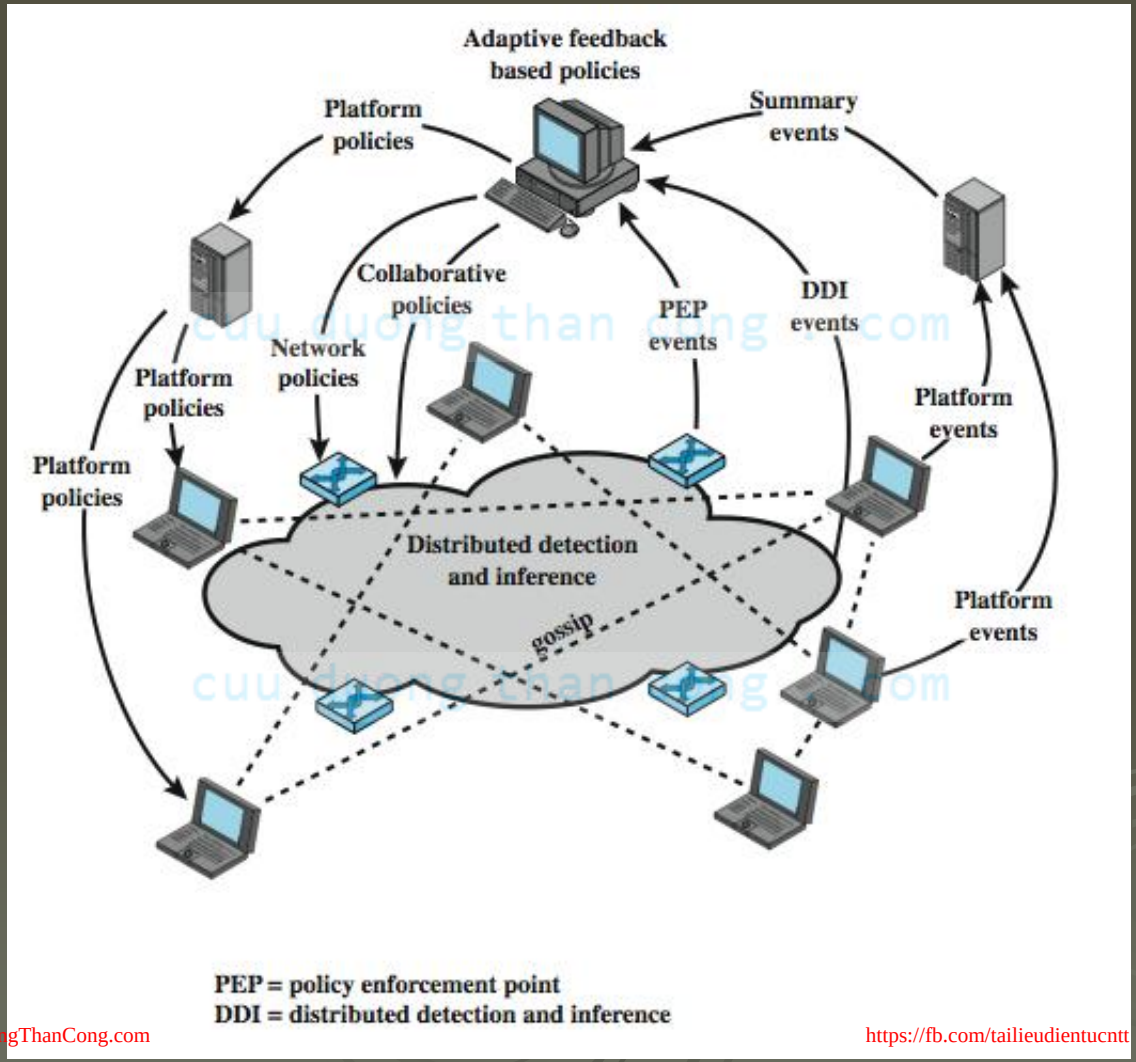
NIDS Sensor Deployment



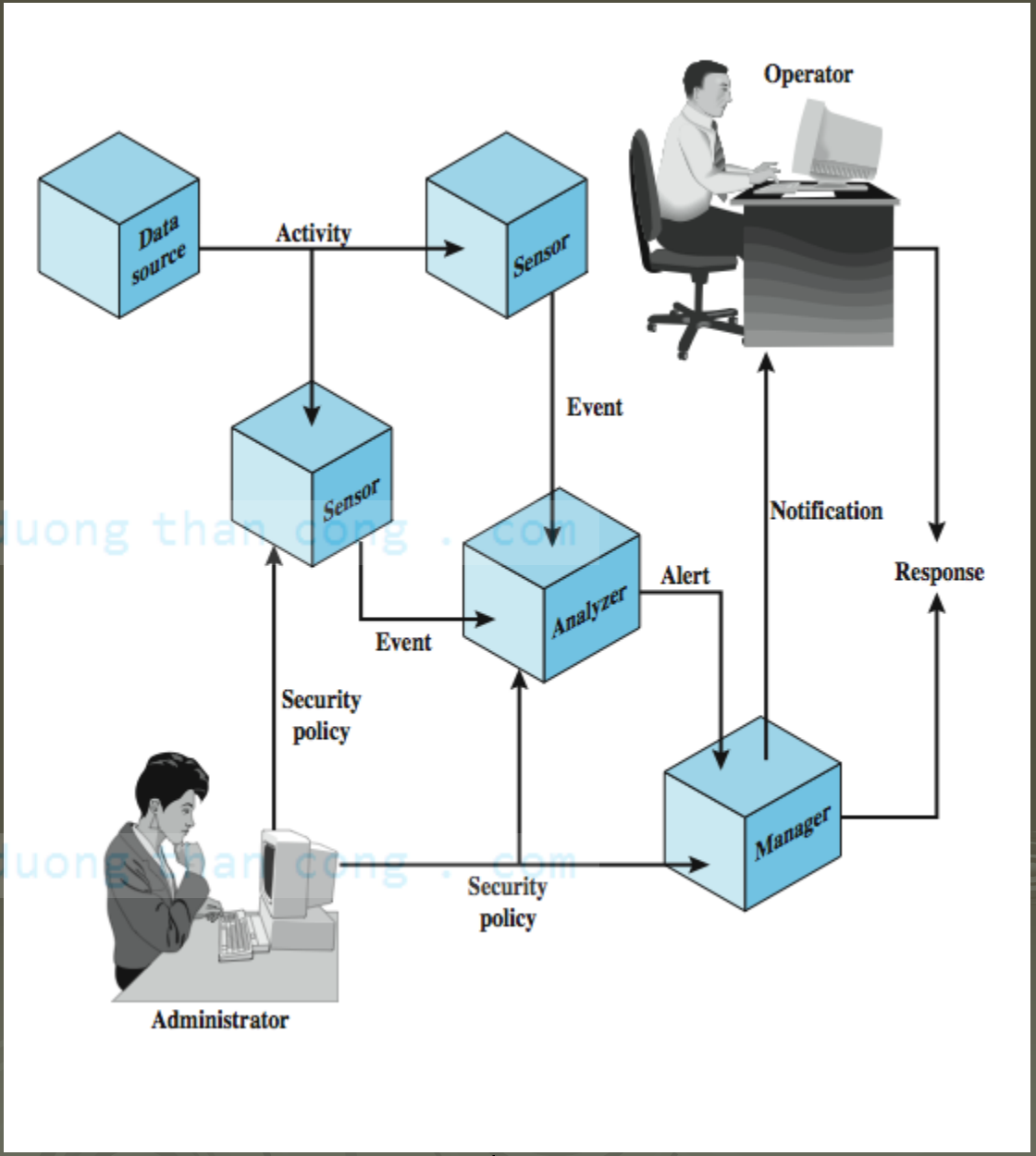
Intrusion Detection Techniques

- signature detection
  - at application, transport, network layers; unexpected application services, policy violations
- anomaly detection
  - of denial of service attacks, scanning, worms
- when potential violation detected sensor sends an alert and logs information
  - used by analysis module to refine intrusion detection parameters and algorithms
  - by security admin to improve protection

Distributed Adaptive Intrusion Detection



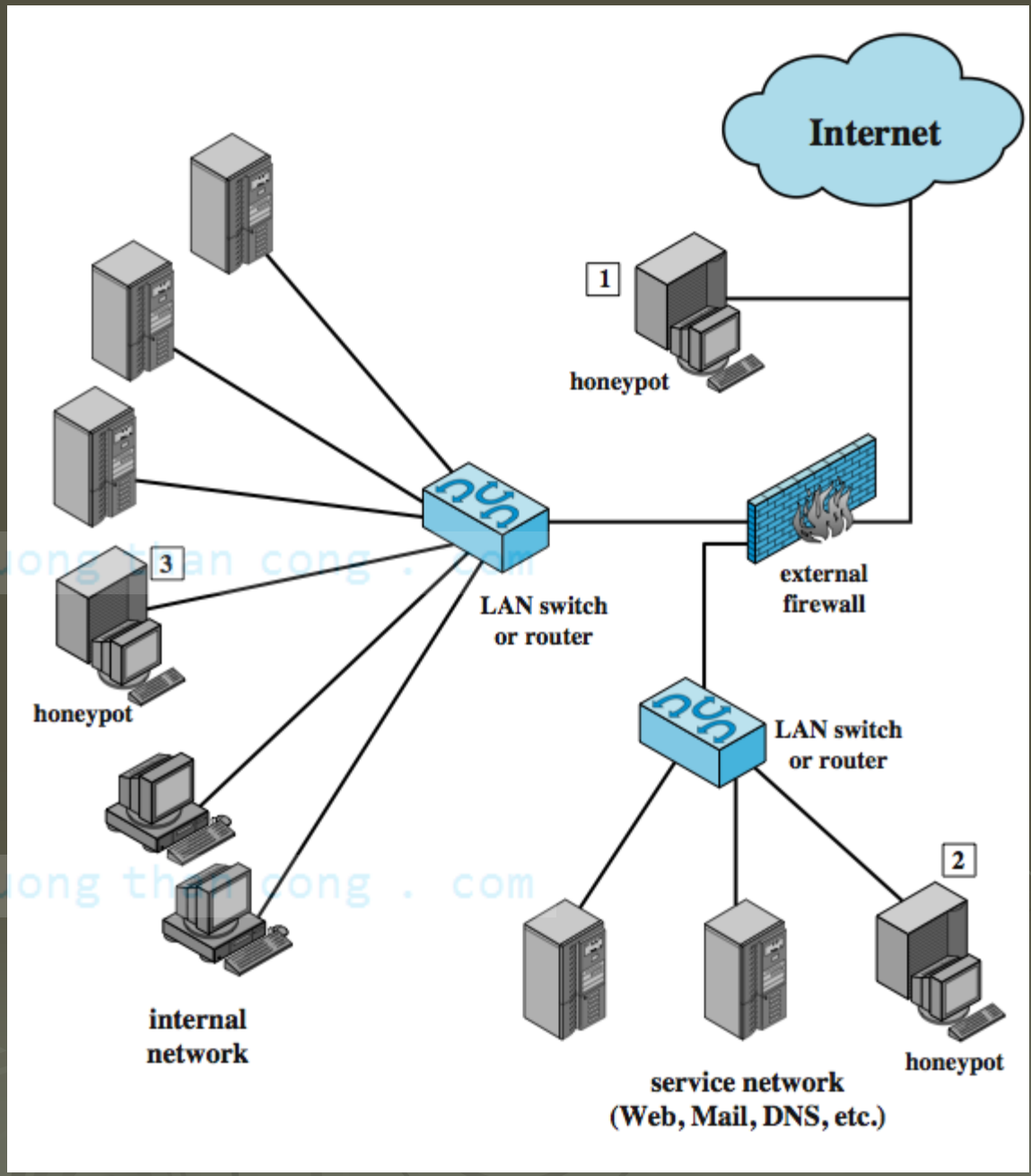
Intrusion Detection Exchange Format



Honeypots

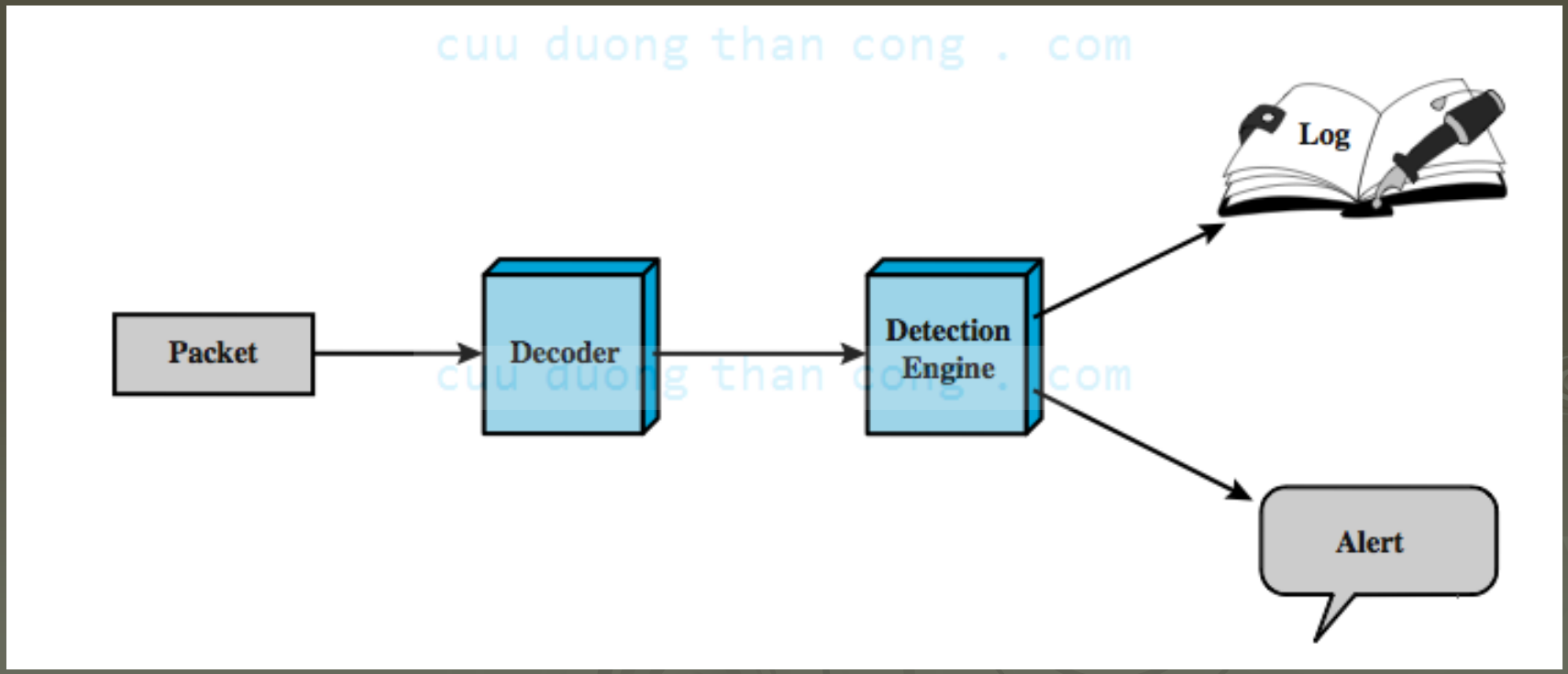
- are decoy systems
  - filled with fabricated info
  - instrumented with monitors / event loggers
  - divert and hold attacker to collect activity info
  - without exposing production systems
- initially were single systems
- more recently are/emulate entire networks

Honeypot Deployment



SNORT

- lightweight IDS
  - real-time packet capture and rule analysis
  - passive or inline



SNORT Rules

- use a simple, flexible rule definition language
- with fixed header and zero or more options
- header includes: action, protocol, source IP, source port, direction, dest IP, dest port
- many options
- example rule to detect TCP SYN-FIN attack:

```
Alert tcp $EXTERNAL_NET any -> $HOME_NET any \
(msg: "SCAN SYN FIN"; flags: SF, 12; \
reference: arachnids, 198; classtype: attempted-recon;)
```

Summary

- introduced intruders & intrusion detection
  - hackers, criminals, insiders
- intrusion detection approaches
  - host-based (single and distributed)
  - network
  - distributed adaptive
  - exchange format
- honeypots
- SNORT example

cuu duong than cong . com