Computer Security DD2395

http://www.csc.kth.se/utbildning/kth/kurser/DD2395/dasakh11/

Fall 2011

Sonja Buchegger
buc@kth.se

Lecture 5

Intrusion Detection

Course Info

- International Students: Oral Exam December, signup on course web site
- Master's:
  - Gpg lab ongoing, server outage today, Nov. 7, ca. 17.30-18.30. If you have unfinished submissions started before that, you might have to submit your key again.
  - Iptables lab signup opened.
  - Web attacks: prepare Gruyere/Webgoat
  - Seminar: form groups, signup for slots. If you need a partner, come to the front in the lecture break.

Computer Security

- Prevention
- Detection
- Response/Recovery

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
- 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.

Hackers

- Often 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

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

Criminal Enterprise

- organized groups of hackers now a threat
  - corporation / government / loosely affiliated gangs
  - 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

- act quickly and precisely to make their activities harder to detect
- exploit perimeter via vulnerable ports
- use trojan horses (hidden software) to leave back doors for re-entry
- use sniffers to capture passwords
- do not stick around until noticed
- 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

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

Intrusion Techniques

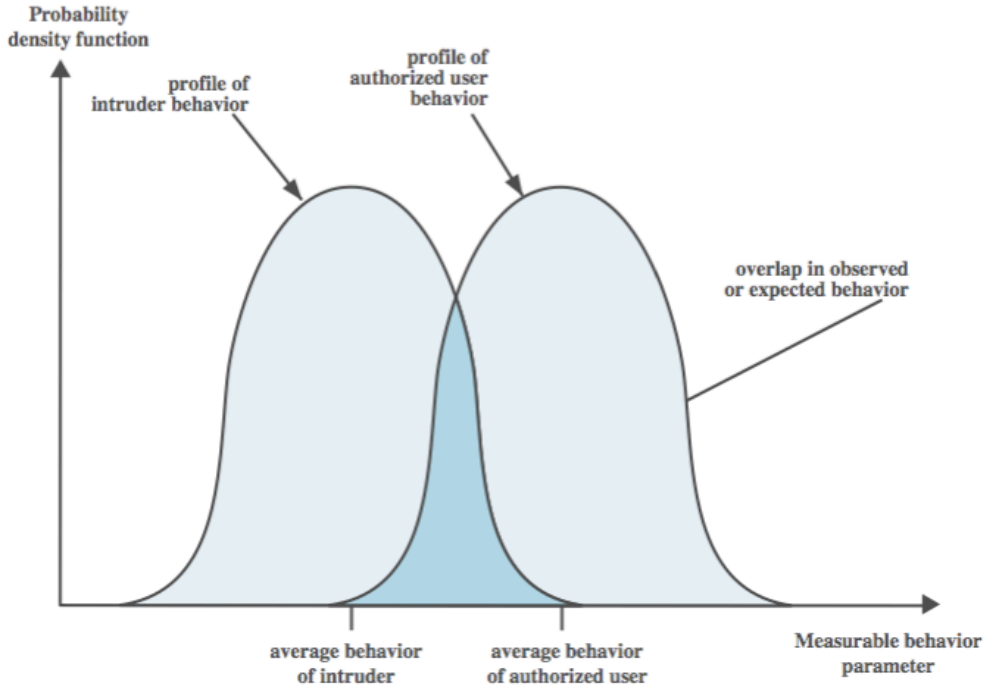
- objective to gain access or increase privileges
- initial attacks often exploit system or software vulnerabilities to execute code to get backdoor
  - e.g. buffer overflow
- or to gain protected information
  - e.g. password guessing or acquisition

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



Test Accuracy

- Example: Test 87% accurate (if one has the disease, the test is positive with 87% probability, if one does not have it, the test is negative with 97% probability).
- 1 in 100 has the disease
- Test comes back positive
- What is the chance of patient NOT having the disease?

Test Accuracy

- 87% accuracy, 1 in 100 has the disease, test comes back positive
- What is the chance of patient NOT having the disease?
- A) 13 %
- B) 50 %
- C) 93,7 %

Base-Rate Fallacy

- Bayes: $P(B|A) = \frac{P(A|B)/P(B)}{P(A)}$

- $P(well|pos) = \frac{P(pos|well)\ P(well)}{P(pos|disease)\ P(disease) + P(pos|well)\ P(well)}$

$\frac{0.13 \times 0.99}{0.87 \times 0.01 + 0.13 \times 0.99} = 0.973$

Base-Rate Fallacy

- Better test: 99.9% - false positive rate: 9%
- Incidence: only 1 in 10 000 – false positive rate: 91%

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

Difficult Task

- Defense has to work all the time, attack only once

For stories about intrusions, penetration testing, see Kevin Mitnick “The Art of Intrusion”

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

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

What if…

- You are being hacked while training the system?
- There is a new normal? Difference between abnormal normal and actual attack?

Signature Detection

- observe events on system and applying a set of rules to decide if intruder
  - rule-based penetration identification
    - rules identify known penetrations / weaknesses
    - often by analyzing attack scripts from Internet
    - supplemented with rules from security experts

Question:

- Signature-based IDS: more likely to have

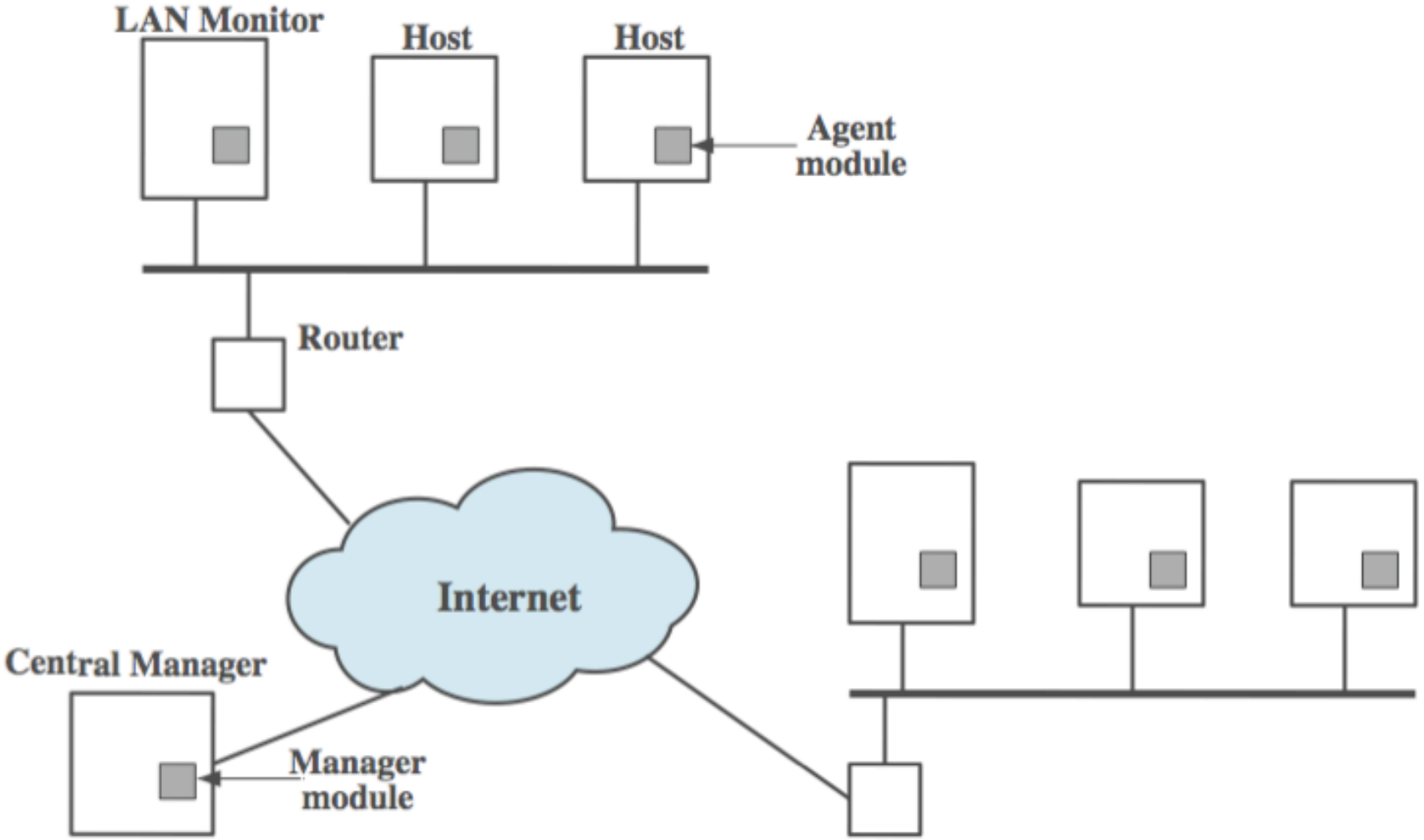
A) false positives or

B) false negatives?

- How about anomaly-based IDS?

A)? B)?

Distributed Host-Based IDS



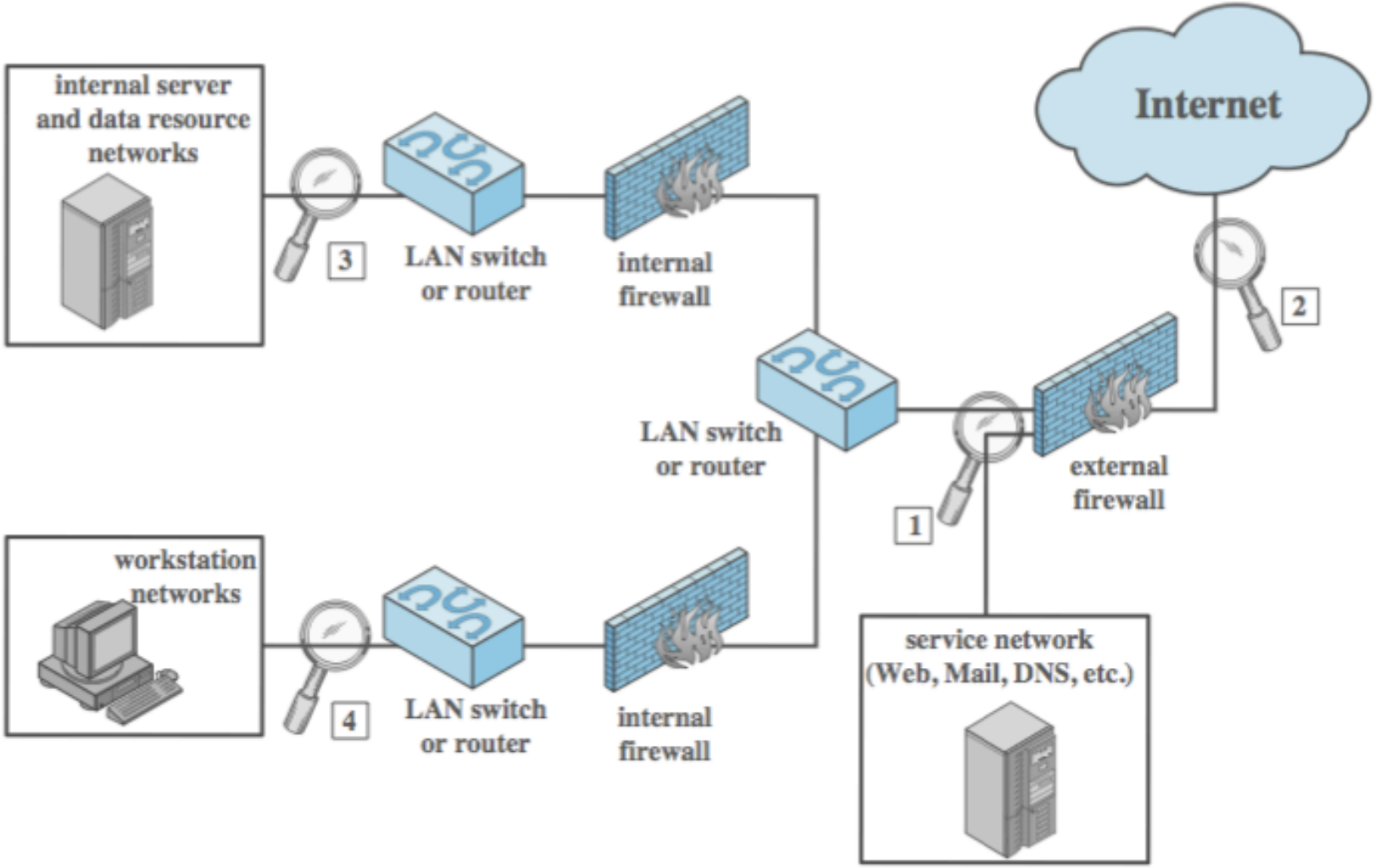
Distributed Host-Based IDS

- Different audit record formats
- Collection point in network, need to transfer raw data or summaries – confidentiality, integrity
- Centralized vs. decentralized architecture

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)

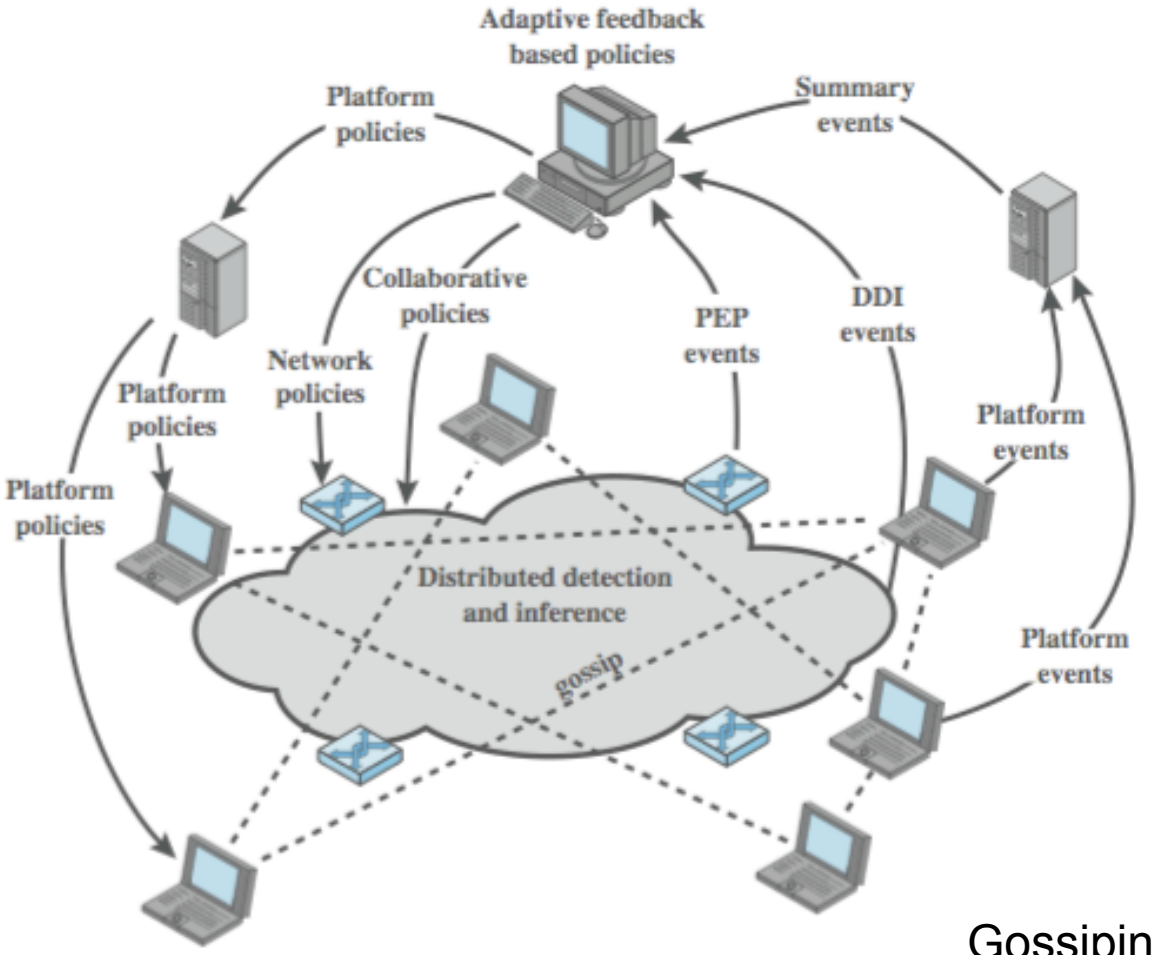
NIDS Sensor Deployment



Intrusion Detection Techniques

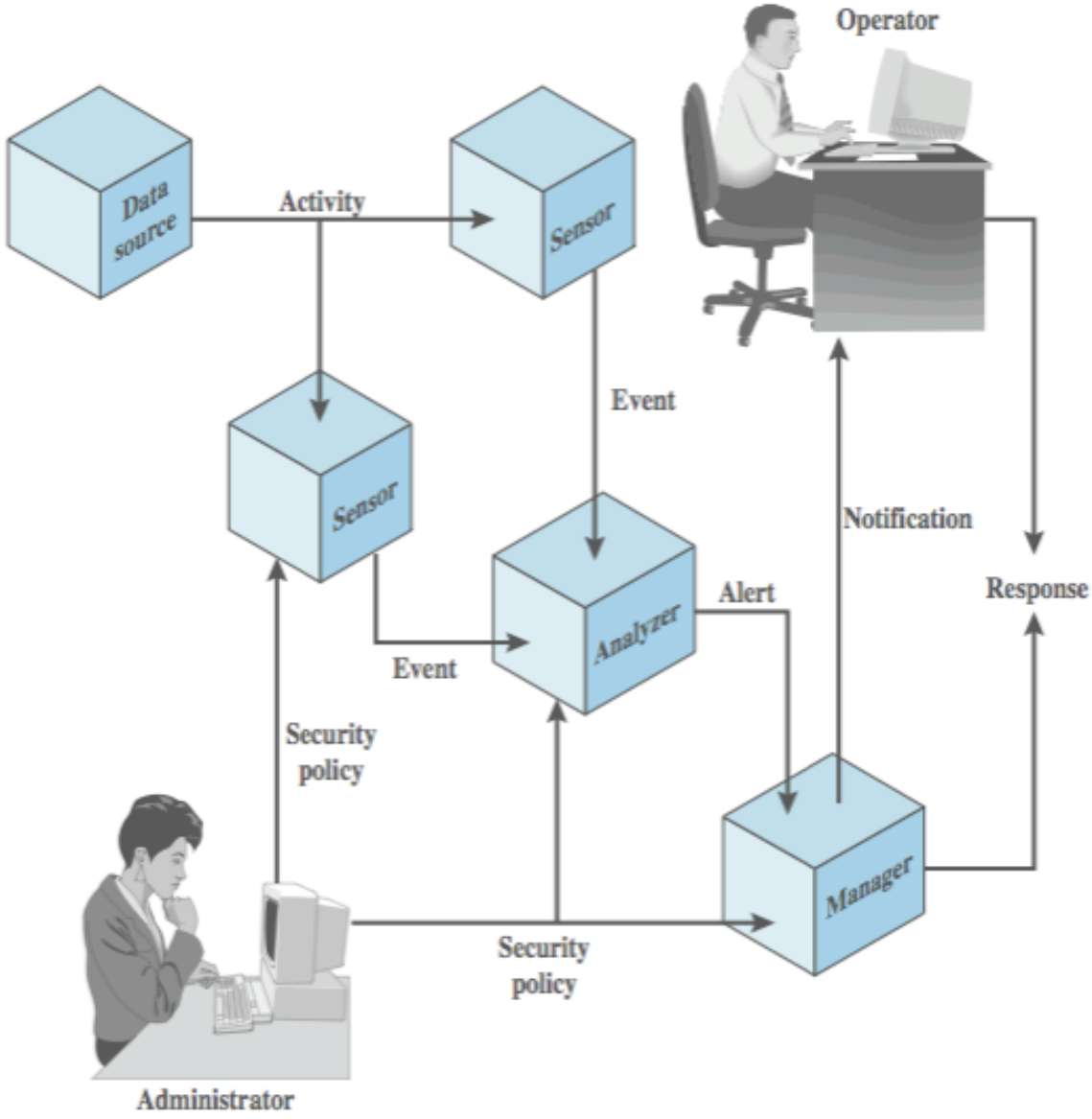
- signature detection
  - at application, transport, network layers; unexpected application services, policy violations
- anomaly detection
  - of denial of service attacks, scanning, worms
- when potential violation detected sensor sends an alert and logs information
  - used by analysis module to refine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

Distributed Adaptive Intrusion Detection



Gossiping: trade #sources for time; helps against stealth

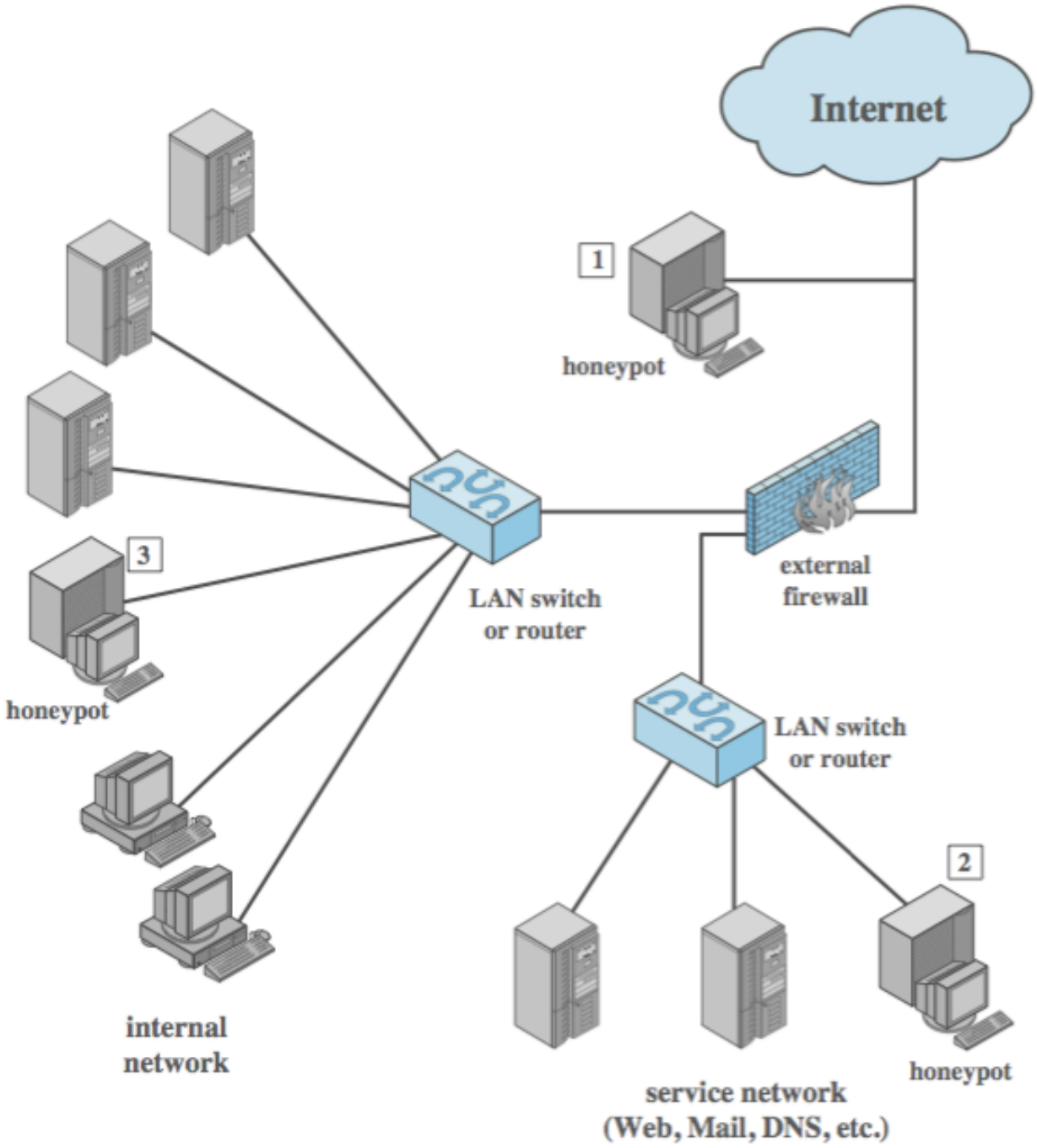
Intrusion Detection Exchange Format



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

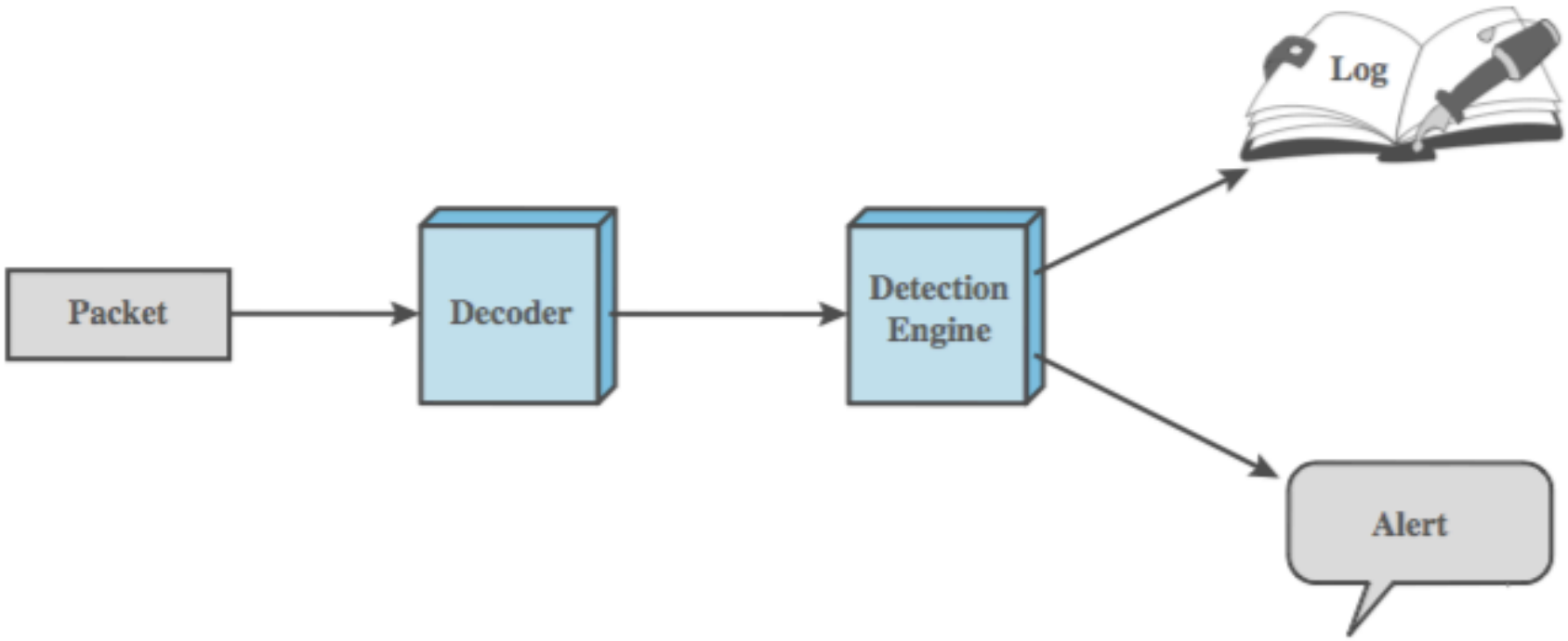
Honeypot Deployment



Risks of Honeypots?

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;)
```

Limitations of Intrusion Detection

See Ross Anderson's book:

- Detecting viruses as hard as the halting problem
- 2 types of intrusions: error-causing or not
- Response can lead to DoS
- False alarms, users/attackers get around them
- Rules: discrimination, data protection law: citizens are entitled to know the algorithms used to process their personal data

Limitations of Intrusion Detection

- NW: Internet is noisy (bugs, out-of-date DNS), leads to false positives
- “too few attacks” – base rate fallacy
- Version-specific attacks, constant need for updates
- Due diligence only, lack of updates
- Encrypted traffic hard to analyze
- Trade-offs, as in firewalls, low-level analysis fast but can have fragmentation, higher-level intensive and frequent updates
- Stealthy attacks

Summary

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