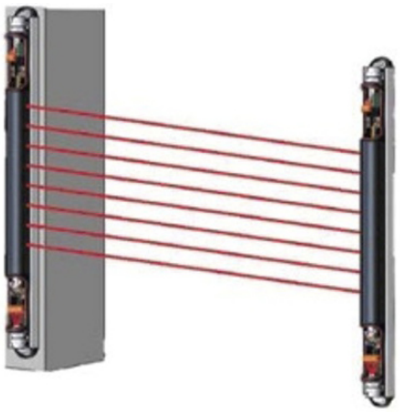
Intrusion Detection



CS 458: Information Security

Kevin Jin

Administrivia

- Homework 11 solution and Homework 12 released
- Quiz 4 due on Nov 22
- Final Exam
  - Date/Time: Dec 2, Regular class time
  - Exam Review on Nov 30

Reading Material

- Chapter 8 of the text

Some materials borrowed from Mark Stamp at San Jose State University

Outline

- What are intrusions?
- Host-based vs. Network-based Intrusion Detection
- Signature-based vs. Anomaly-based Intrusion Detection

What is an Intrusion?

- An unauthorized entity attempts to gain access to a protected resource

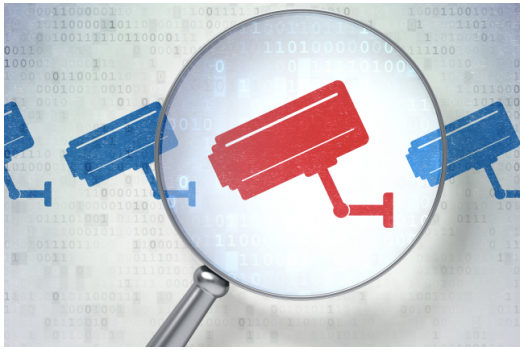
- Examples
  - Root compromise
  - Privilege escalation

Intrusion Prevention

- Want to keep bad guys out
- **Intrusion prevention** is a traditional focus of computer security
  - Authentication is to prevent intrusions
  - Firewalls a form of intrusion prevention
  - Virus defenses aimed at intrusion prevention
  - Like locking the door on your car

Intrusion Detection

- In spite of intrusion prevention, bad guys will sometimes get in
- Intrusion detection systems (**IDS**)
  - Detect attacks in progress (or soon after)
  - Look for unusual or suspicious activity
- IDS evolved from log file analysis
- How to respond when intrusion detected?
  - alerting administrators via email/pager/phone
  - changing firewall configurations
  - …



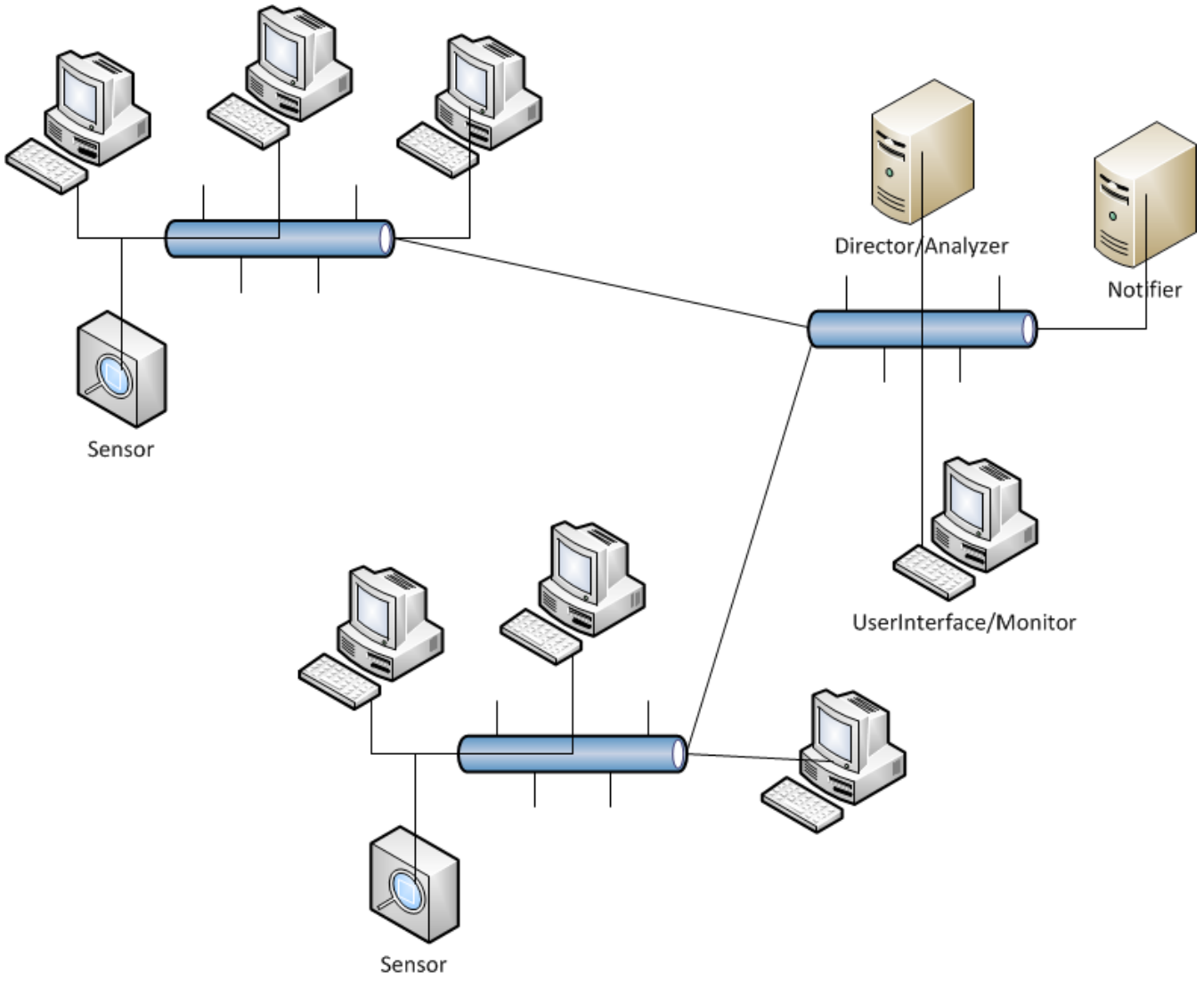
Intrusion Detection Systems

- Who is likely intruder?
  - May be outsider who got through firewall
  - May be evil insider
- What do intruders do?
  - Launch well-known attacks
  - Launch variations on well-known attacks
  - Launch new/little-known attacks
  - "Borrow" system resources
  - Use compromised system to attack others. etc.

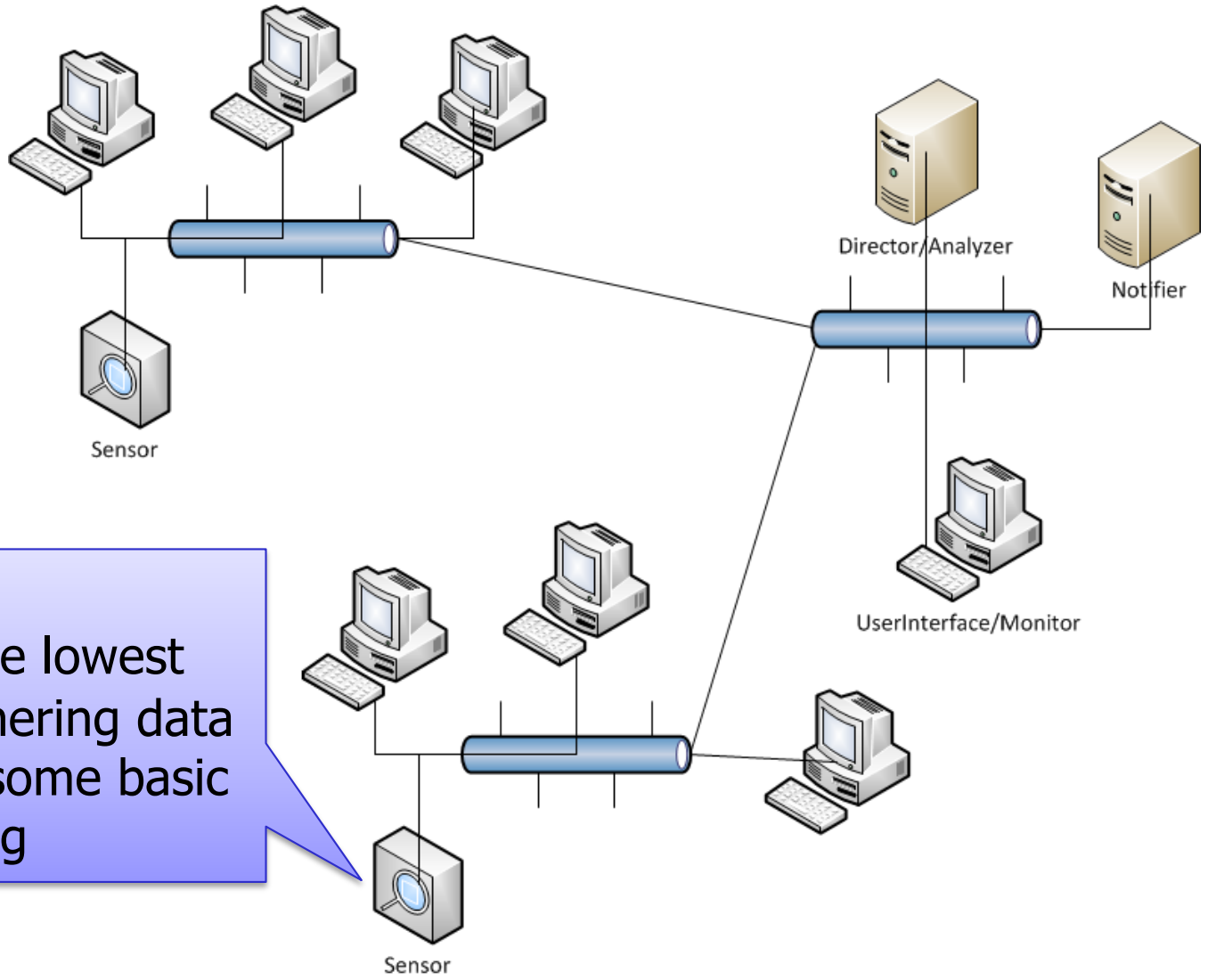
Bad Detections

- False Positive
  - Detect activity as an intrusion, but it isn't
  - Reduce by loosening intrusion detection rules
- False Negative
  - Miss reporting bad behavior as an intrusion
  - Reduce by tightening intrusion detection rules

IDS Elements

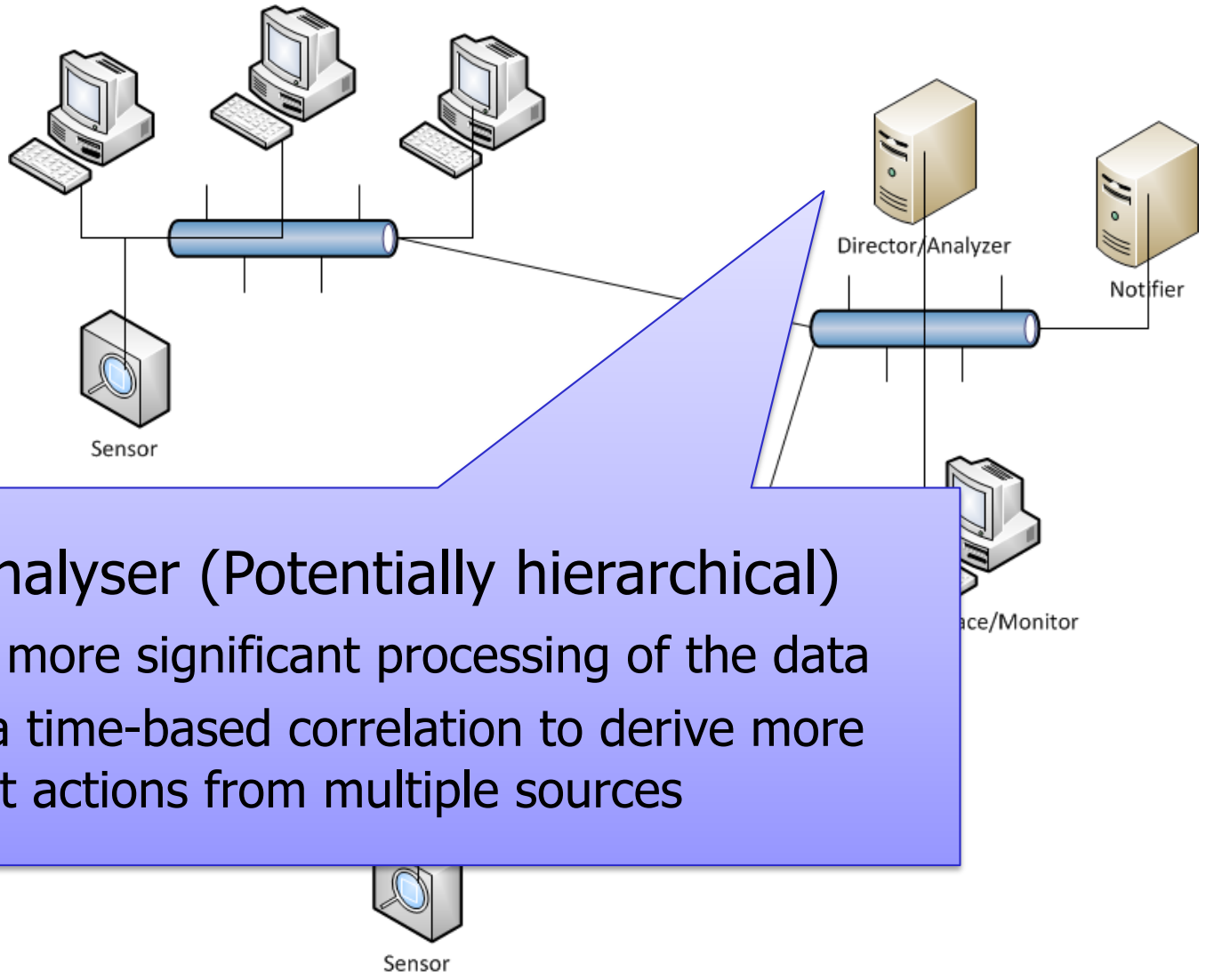


IDS Elements



Sensors
- Run at the lowest level gathering data
- Perform some basic processing

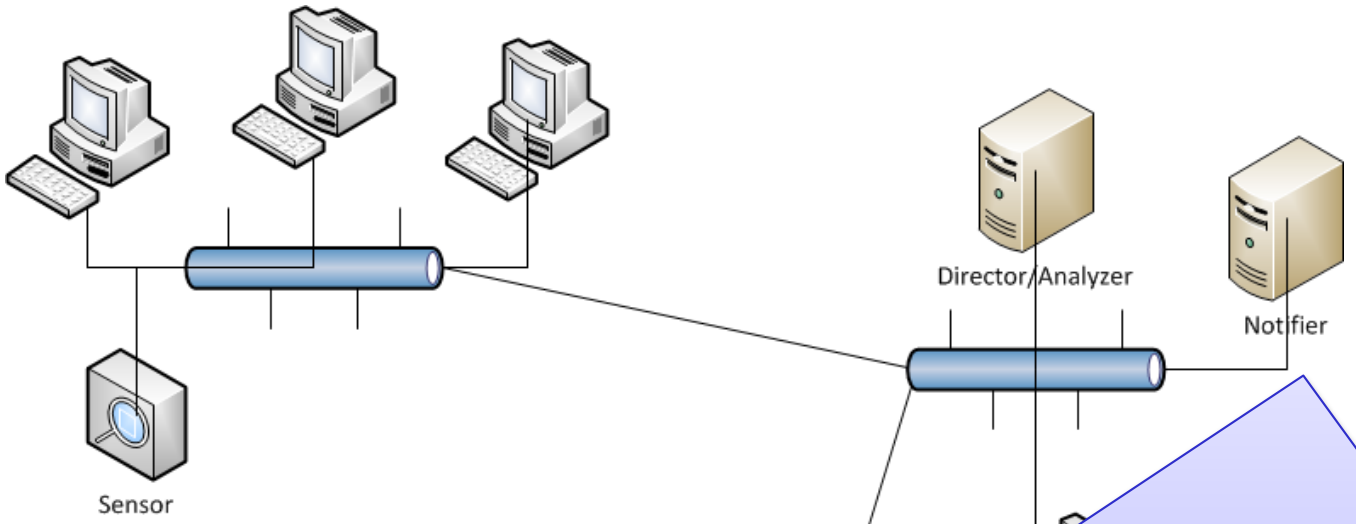
IDS Elements



Director/analyser (Potentially hierarchical)

- performs more significant processing of the data
- perform a time-based correlation to derive more significant actions from multiple sources

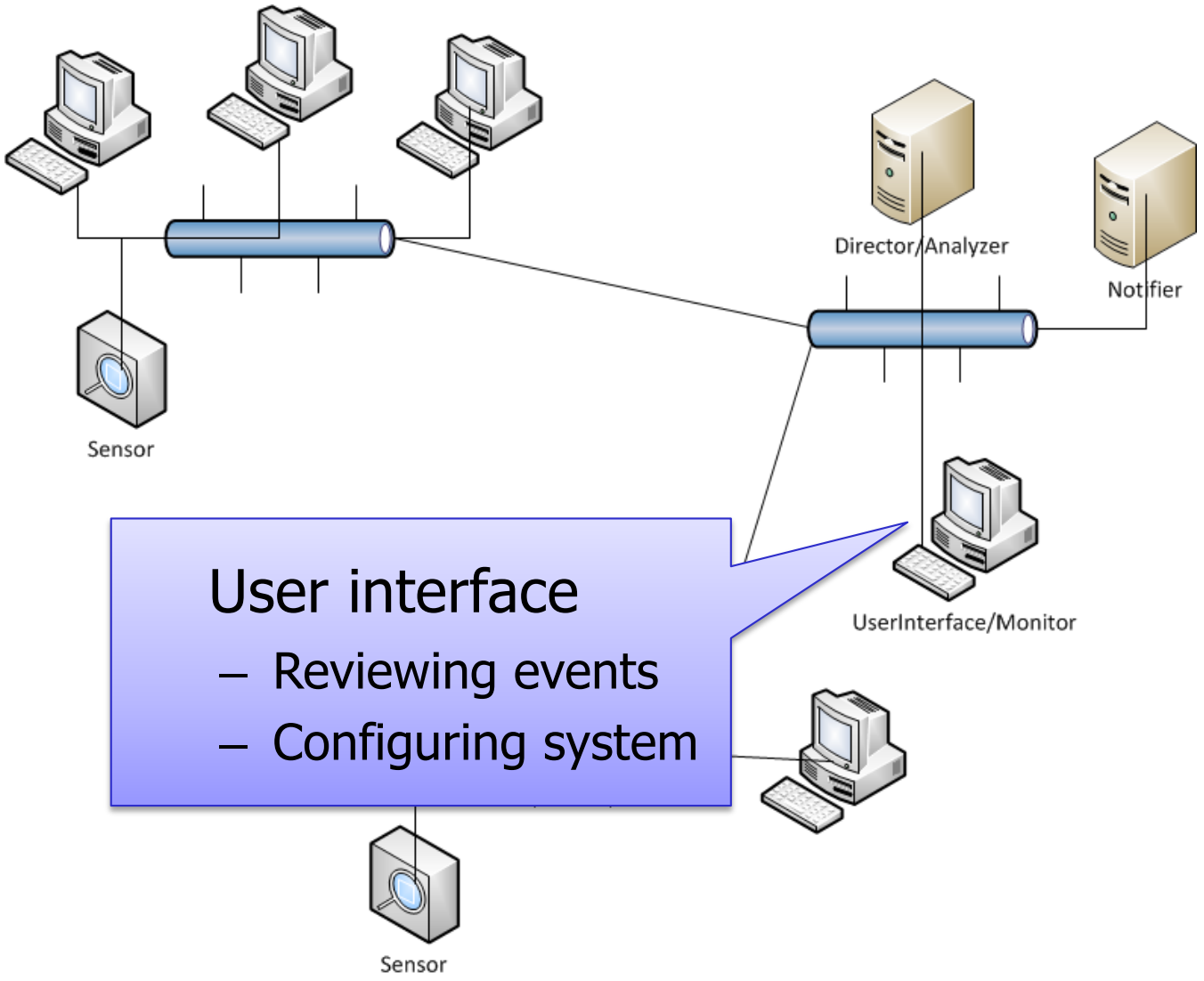
IDS Elements



Notifiers: perform some action in response to a detected attack

- Popup a window on a screen
- Send an email or a page
- Send a new syslog message elsewhere
- Adjust a firewall or some other policy to block future action from the attacker

IDS Elements



User interface
- Reviewing events
- Configuring system

Data Sources

- Direct data
  - Network packets
  - System calls
- Indirect data
  - Syslog data, Windows event logs
  - Events from other intrusion detection systems
  - Netflow information generated by routers about network traffic

IDS

- Intrusion detection **approaches**
  - Signature-based IDS
  - Anomaly-based IDS
- Intrusion detection **architectures**
  - Host-based IDS
  - Network-based IDS
- Any IDS can be classified as above
  - In spite of marketing claims to the contrary!

Host-Based IDS

- Monitor activities on hosts for
  - Known attacks
  - Suspicious behavior
- Designed to detect attacks such as
  - Buffer overflow
  - Escalation of privilege, …
- Little or no view of network activities

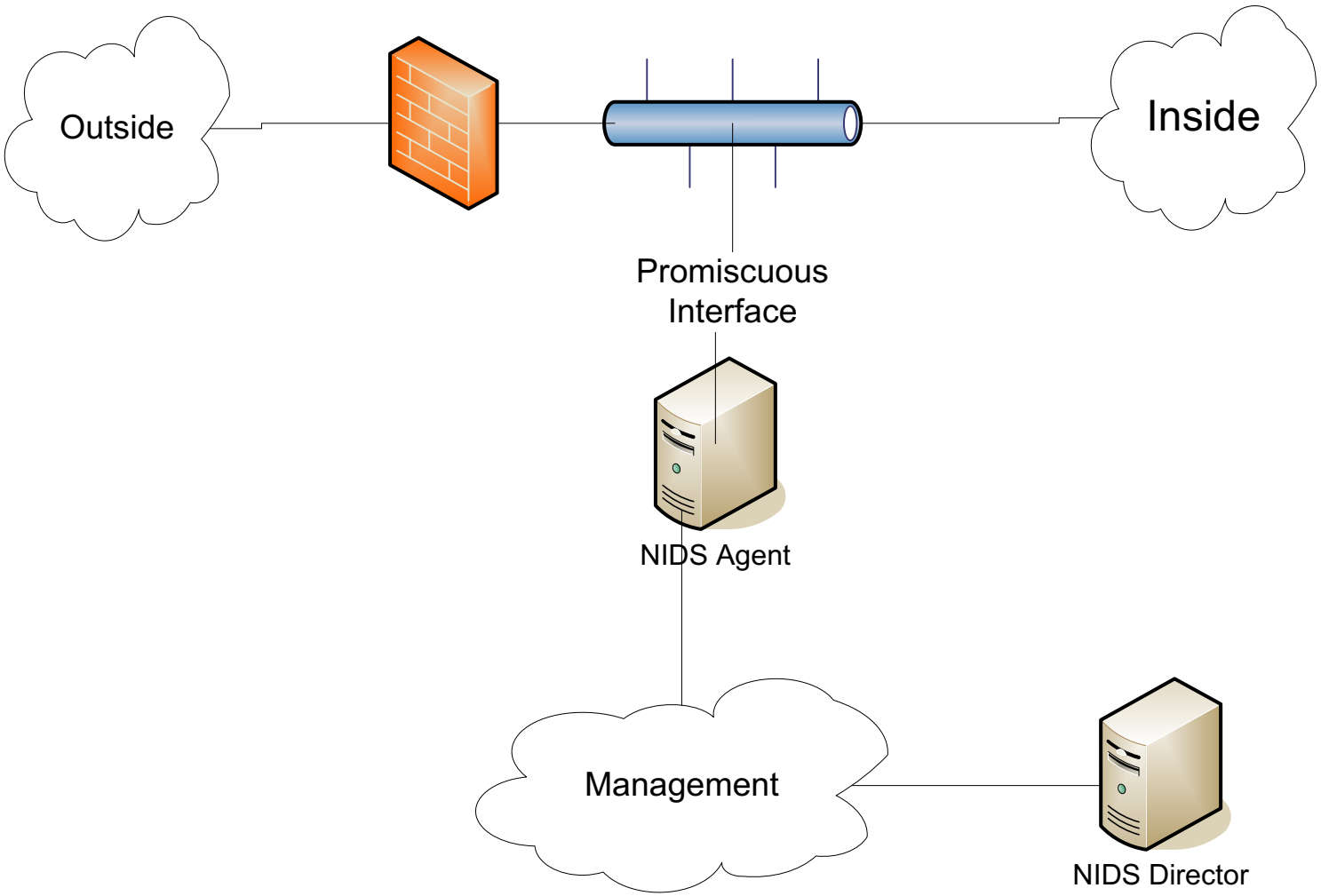
Host Based IDS Examples

- Tripwire – Very basic detection of changes to installed binaries
- More recent HIDS. Look at patterns of actions of system calls, file activity, etc. to permit, deny, or query operations
  - Cisco Security Agent
  - Symantec
  - McAfee Entercept

Network-Based IDS

- Monitor activity on the network for…
  - Known attacks
  - Suspicious network activity
- Designed to detect attacks such as
  - Denial of service
  - Network probes
  - Malformed packets, etc.
- Some overlap with firewall
- Little or no view of host-base attacks
- Can have both host and network IDS

Classical NIDS deployment



NIDS Remediation Options

- Log the event
  - Send text or email
- Reset the connection
- Change the configuration of a nearby router or firewall to block future connections

Signature Detection Example

- Failed login attempts may indicate password cracking attack
- IDS could use the rule "N failed login attempts in M seconds" as **signature**
- If N or more failed login attempts in M seconds, IDS warns of attack
- Note that such a warning is specific
  - Admin knows what attack is suspected
  - Easy to verify attack (or false alarm)

Signature Detection

- Suppose IDS warns whenever N or more failed logins in M seconds
  - Set N and M so false alarms not common
  - Can do this based on "normal" behavior
- But, if Eve knows the signature, he/she can try $N - 1$ logins every M seconds…
- Then signature detection slows down Eve, but might not stop him/her

Signature Detection

- Many techniques used to make signature detection more robust
- Goal is to detect "almost" signatures
- For example, if "about" N login attempts in "about" M seconds
  - Warn of possible password cracking attempt
  - What are reasonable values for "about"?
  - Can use statistical analysis, heuristics, etc.
  - Must not increase false alarm rate too much

Example Signature

- Signature for port sweep
  - A set of TCP packets attempting to connect to a sequence of ports on the same device in a fixed amount of time
- In some environments, the admin might run nmap periodically to get an inventory of what is on the network
  - You would not want to activate this signature in that case

Signature Detection

- Advantages of signature detection
  - Simple
  - Detect known attacks
  - Know which attack at time of detection
  - Efficient (if reasonable number of signatures)
- Disadvantages of signature detection
  - Signature files must be kept up to date
  - Number of signatures may become large
  - Can only detect known attacks
  - Variation on known attack may not be detected

Anomaly Detection

- Anomaly detection systems look for unusual or abnormal behavior
- There are (at least) two challenges
  - What is normal for this system?
  - How "far" from normal is abnormal?
- No avoiding statistics here!
  - **mean** defines normal
  - **variance** gives distance from normal to abnormal

How to Measure Normal?

- Must measure during "representative" behavior
- Must not measure during an attack…
- …or else attack will seem normal!
- Normal is statistical **mean**
- Must also compute **variance** to have any reasonable idea of abnormal

How to Measure Abnormal?

- Abnormal is relative to some "normal"
  - Abnormal indicates possible attack
- Statistical discrimination techniques include
  - Bayesian statistics
  - Linear discriminant analysis (LDA)
  - Quadratic discriminant analysis (QDA)
  - Neural nets, hidden Markov models (HMMs), etc.
- Fancy modeling techniques also used
  - Artificial intelligence
  - Artificial immune system principles
  - Many, many, many others

Anomaly Detection (1)

- Suppose we monitor use of three commands:

  open, read, close
- Under normal use we observe Alice:

  open, read, close, open, open, read, close, …
- Of the six possible ordered pairs, we see four pairs are normal for Alice,

  (open, read), (read, close), (close, open), (open, open)
- Can we use this to identify unusual activity?

Anomaly Detection (1)

- We monitor use of the three commands

  $\text{open}, \text{read}, \text{close}$

- If the ratio of abnormal to normal pairs is "too high", warn of possible attack
- How could we improve this approach?
  - Also use expected frequency of each pair
  - Use more than two consecutive commands
  - Include more commands/behavior in the model
  - More sophisticated statistical discrimination

Anomaly Detection (2)

- Over time, Alice has accessed file F_n at rate H_n

H_0	H_1	H_2	H_3
.10	.40	.40	.10

- Recently, "Alice" has accessed F_n at rate A_n

A_0	A_1	A_2	A_3
.10	.40	.30	.20

- Is this normal use for Alice?
- We compute $S = (H_0 - A_0)^2+(H_1 - A_1)^2+\ldots+(H_3 - A_3)^2 = .02$
  - If we consider $S < 0.1$ to be normal, this is normal
- How to account for use that varies over time?

Anomaly Detection (2)

- To allow "normal" to adapt to new use, we update averages: $H_n = 0.2A_n + 0.8H_n$
- In this example, H_n are updated
  $H_2 = 0.2 * 0.3 + 0.8 * 0.4 = 0.38$ and
  $H_3 = 0.2 * 0.2 + 0.8 * 0.1 = 0.12$
- And we now have

H_0	H_1	H_2	H_3
.10	.40	.38	.12

Anomaly Detection (2)

- The updated long term average is

H_0	H_1	H_2	H_3
.10	.40	.38	.12

- Suppose new observed rates…

A_0	A_1	A_2	A_3
.10	.30	.30	.30

- Is this normal use?
- Compute $S = (H_0 - A_0)^2 + \ldots + (H_3 - A_3)^2 = .0488$
  - Since $S = .0488 < 0.1$, we consider this normal
- And we again update the long term averages:

$$H_n = 0.2A_n + 0.8H_n$$

Anomaly Detection (2)

- The starting averages were:

H_0	H_1	H_2	H_3
.10	.40	.40	.10

- After 2 iterations, averages are:

H_0	H_1	H_2	H_3
.10	.38	.364	.156

- Statistics slowly evolve to match behavior
- This reduces false alarms
- But also opens an avenue for attack…
  - Suppose Eve **always** wants to access F_3
  - Can he/she convince IDS this is normal for Alice?

Anomaly Detection Issues

- Systems constantly evolve and so must IDS
  - Static system would place huge burden on admin
  - But evolving IDS makes it possible for attacker to (slowly) convince IDS that an attack is normal
  - Attacker may win simply by "going slow"
- What does "abnormal" really mean?
  - Indicates there **may be** an attack
  - Might not be any specific info about "attack"
  - How to respond to such vague information?
  - In contrast, signature detection is very specific

Anomaly Detection

- Advantages?
  - Chance of detecting unknown attacks
- Disadvantages?
  - Cannot use anomaly detection alone…
  - … must be used with signature detection
  - Reliability is unclear
  - May be subject to attack
  - Anomaly detection indicates "something unusual", but lacks specific info on possible attack

Anomaly Detection the Bottom Line

- Anomaly-based IDS is active research topic
- Many security experts have high hopes for its ultimate success
- Often cited as key future security technology
- Hackers are not convinced!
  - Title of a talk at Defcon: "Why Anomaly-based IDS is an Attacker's Best Friend"
- Anomaly detection is difficult and tricky
- As hard as AI?

Summary

- Detecting intrusions accurately enough is difficult
- Dynamic IDS is necessary to keep up with attackers
- IDS can be applied to hosts and networks