Intrusion Detection

Raj Jain
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@cse.wustl.edu

Audio/Video recordings of this lecture are available at:

http://www.cse.wustl.edu/~jain/cse571-17/

Overview

1. Intruders
2. Intrusion Detection
3. Password Management

These slides are based partly on Lawrie Brown's slides supplied with William Stallings's book "Cryptography and Network Security: Principles and Practice," 7th Ed, 2017.

Concepts

- **Threat**: Party that exploits a vulnerability
- **Structured Threat**: Adversaries with a formal methodology, a financial sponsor, and a defined objective.
- **Unstructured Threat**: Compromise victims out of intellectual curiosity

Intrusion vs. Extrusion Detection

- **Intrusion Detection**: Detecting unauthorized activity by inspecting inbound traffic
- **Extrusion Detection**: Detecting unauthorized activity by inspecting outbound traffic
- **Extrusion**: Insider visiting malicious web site or a Trojan contacting a remote internet relay chat channel

Categories of Intruders

- **Hackers**: Motivated by thrill of access and status
  - Hacking community a strong meritocracy
  - Status is determined by level of competence
  - Computer Emergency Response Teams (CERTs) -Collect / disseminate vulnerability info / responses
- **Criminal Enterprises**: Organized groups of hackers
  - E.g., Eastern European or Russian hackers
  - Often target credit cards on e-commerce server
- **Internal Threat**
  - May be motivated by revenge / entitlement
  - When employment terminated
  - Taking customer data when move to competitor

Ref: http://en.wikipedia.org/wiki/Computer_emergency_response_team

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

Ref: http://en.wikipedia.org/wiki/Hacker_(computer_security)

Criminal Enterprise Behavior

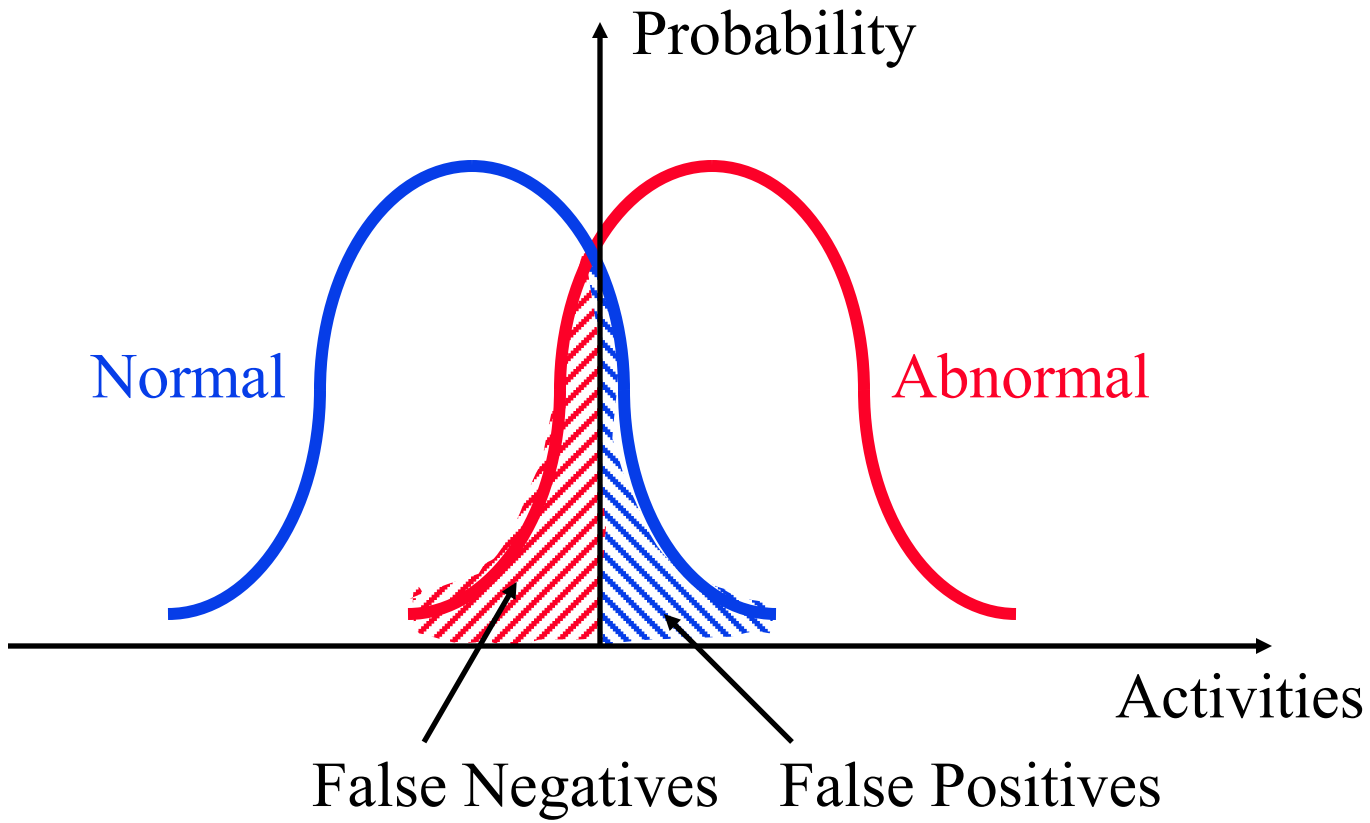
1. Act quickly and precisely to make their activities harder to detect
2. Exploit perimeter via vulnerable ports
3. Use trojan horses (hidden software) to leave back doors for re-entry
4. Use sniffers to capture passwords
5. Do not stick around until noticed
6. Make few or no mistakes.

Insider 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.

Notification Alarms

- False Positive: Valid traffic causes an alarm
- False Negative: Invalid traffic does not cause an alarm



Types of IDS

- **Signature Based IDS**: Search for known attack patterns using pattern matching, heuristics, protocol decode
- **Rule Based IDS**: Violation of security policy
- **Anomaly-Based IDS**
- **Statistical or non-statistical** detection
- Response:
  - **Passive**: Alert the console
  - **Reactive**: Stop the intrusion ⇒ Intrusion Prevention System ⇒ Blocking

Ref: http://en.wikipedia.org/wiki/Intrusion_detection_system, http://en.wikipedia.org/wiki/Intrusion_detection

Sample Signatures

- ICMP Floods directed at a single host
- Connections of multiple ports using TCP SYN
- A single host sweeping a range of nodes using ICMP
- A single host sweeping a range of nodes using TCP
- Connections to multiple ports with RPC requests between two nodes

Rule-Based Intrusion Detection

- Rule-based anomaly detection
  - Analyze historical audit records to identify usage patterns and auto-generate rules for them
- Rule-based penetration identification
  - Uses expert systems technology
  - With rules identifying known penetration, weakness patterns, or suspicious behavior
  - Compare audit records or states against rules
  - Rules usually machine & O/S specific
  - Rules are generated by experts who interview & codify knowledge of security admins
  - Quality depends on how well this is done

Anomaly Based IDS

- Traffic that deviates from normal, e.g., routing updates from a host
- Statistical Anomaly: sudden changes in traffic characteristics
- Machine Learning: Learn from false positives and negatives
- Data Mining: Develop fuzzy rules to detect attacks

Statistical Anomaly Detection

- Threshold detection
  - Count occurrences of specific event over time
  - If exceed reasonable value assume intrusion
  - Used alone, it is a crude and ineffective detector
- Profile based
  - Characterize past behavior of users
  - Detect significant deviations from this
  - Profile usually multi-parameter

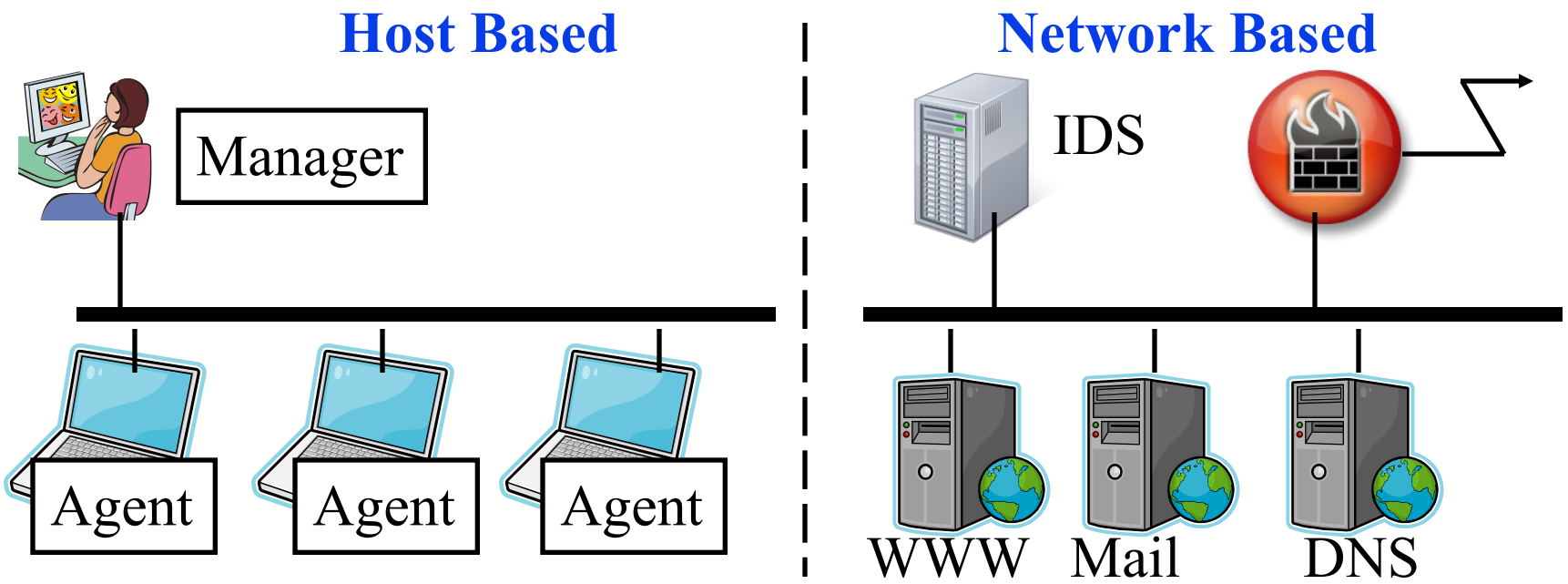
Audit Records

- Fundamental tool for intrusion detection
- Native audit records: Part of all common multi-user O/S
- Detection-specific audit records
  - Created specifically to collect wanted info
- Audit Record Analysis: Foundation of statistical approaches
- Analyze records to get metrics over time
  - Counter, gauge, interval timer, resource use
- Use various tests on these to determine if current behavior is acceptable
  - Mean & standard deviation, multivariate, markov process, time series, operational
- Key advantage is no prior knowledge used

Ref: http://en.wikipedia.org/wiki/Information_security_audit, http://en.wikipedia.org/wiki/Audit_trail

Types of IDS

- IDS Sensor: SW/HW to collect and analyze network traffic
- Host IDS: Runs on each server or host
- Network IDS: Monitors traffic on the network
  Network IDS may be part of routers or firewalls



Ref: http://en.wikipedia.org/wiki/Host-based_intrusion_detection_system
http://en.wikipedia.org/wiki/Network_intrusion_detection_system

Host vs. Network IDS

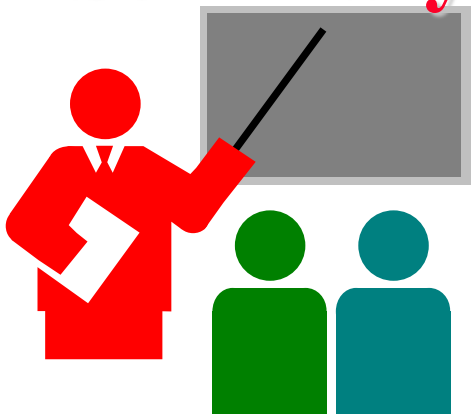
IDS Type	Pros	Cons
Host IDS	Verification of success or failure of an attack possible	OS/HW dependent
	Specific to a system	Impacts performance of the host
	Not limited by network bandwidth or encryption	One per host ⇒ Expensive
Network IDS	Protects all hosts	Challenging to see all traffic in a switched environment
	Independent of OS/HW	Too much traffic to analyze
	Useful against probes and DoS attacks	Not effective against single packet attacks and encrypted traffic

Honeypots

- Decoy systems to lure attackers
  - Away from accessing critical systems
  - To collect information of their activities
  - To encourage attacker to stay on system so administrator can respond
- Are filled with fabricated information
- Instrumented to collect detailed information on attackers activities
- Single or multiple networked systems

Ref: http://en.wikipedia.org/wiki/Honeypot_(computing)

Summary



1. Intruders can be both internal, external or organized
2. IDS can be signature based, anomaly based, or statistical Should minimized false positives and false negatives.
3. IDS can be host based or network based. Host based is more scalable.
4. Honeypots can be used to detect intruders

References

- http://en.wikipedia.org/wiki/Computer_emergency_response_team
- http://en.wikipedia.org/wiki/Hacker_(computer_security)
- http://en.wikipedia.org/wiki/Honeypot_(computing)
- http://en.wikipedia.org/wiki/Host-based_intrusion_detection_system
- http://en.wikipedia.org/wiki/Network_intrusion_detection_system
- http://en.wikipedia.org/wiki/Information_security_audit
- http://en.wikipedia.org/wiki/Audit_trail
- http://en.wikipedia.org/wiki/Intrusion_detection_system
- http://en.wikipedia.org/wiki/Intrusion_detection
- http://en.wikipedia.org/wiki/Password_cracking
- http://en.wikipedia.org/wiki/Salt_(cryptography)
- https://en.wikipedia.org/wiki/Pepper_(cryptography)

Acronyms

- CERT Computer Emergency Response Team
- DES Data Encryption System
- FIPS Federal Information Processing Standard
- FTP File Transfer Protocol
- HW Hardware
- ICMP Internet Control Message Protocol
- ID Intrusion Detection
- IDS Intrusion Detection System
- IETF Internet Engineering Task Force
- IP Internet Protocol
- IPS Intrusion prevention systems
- MD5 Message Digest 5
- RPC Remote Procedure Call
- SW Software
- SYN Synchronization
- TCP Transmission Control Protocol
- WWW World Wide Web

Scan This to Download These Slides

Raj Jain
http://rajjain.com

Related Modules

CSE571S: Network Security (Spring 2017),
http://www.cse.wustl.edu/~jain/cse571-17/index.html

CSE473S: Introduction to Computer Networks (Fall 2016),
http://www.cse.wustl.edu/~jain/cse473-16/index.html

Wireless and Mobile Networking (Spring 2016),
http://www.cse.wustl.edu/~jain/cse574-16/index.html

CSE571S: Network Security (Fall 2014),
http://www.cse.wustl.edu/~jain/cse571-14/index.html

Audio/Video Recordings and Podcasts of
Professor Raj Jain's Lectures,
https://www.youtube.com/channel/UCN4-5wzNP9-ruOzQMs-8NUw