

Intrusion Detection Systems



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/cse571-07/>



- Concepts
- Intrusion vs. Extrusion Detection
- Types of IDS
- Host vs. Network IDS
- Protocols for IDS: Syslog, BEEP, IDXP

Concepts

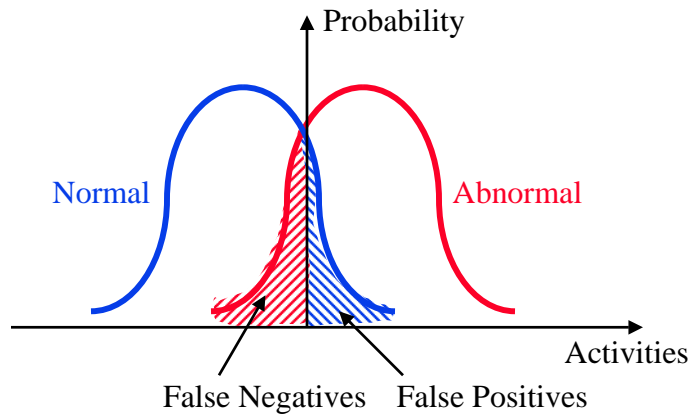
- ❑ **Intrusion:** Break into, misuse, or exploit a system (against policy)
- ❑ **Intruders:** Insiders or outsiders
Most IDS are designed for outsiders
- ❑ **Vulnerability:** Weakness that could be used by the attacker
- ❑ **Threat:** Party that exploits a vulnerability
- ❑ **Structured Threat:** Adversaries 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

Notification Alarms

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



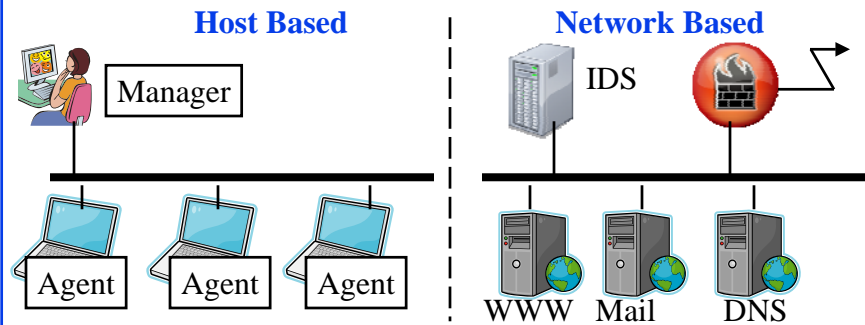
23-5

Types of IDS Sensors

- ❑ Log analyzers: Matching log entry \Rightarrow Action
- ❑ Signature based sensors
- ❑ System call analyzers: Shim between applications and OS
- ❑ Application behavior analyzers: E.g., web server writing a file
- ❑ File Integrity checkers

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



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 |

Types of IDS (Cont)

- ❑ 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

Signature Based IDS

- ❑ 5-tuple packet filtering (SA/DA/L4 protocol/ports)
- ❑ Use Ternary Content Addressable Memories (TCAMs)
- ❑ Deep packet inspection requires pattern string matching algorithms (Aho-Corasik algorithm and enhancements)
- ❑ Regular expression signatures

Types of Signatures

| Category | Types |
|----------|--|
| IP | IP Options IP Fragmentation Bad IP packets |
| ICMP | ICMP Traffic Records Ping Sweeps ICMP attacks |
| TCP | TCP Traffic Records TCP Port Scans TCP host Sweeps Mail attacks |
| ... | ... |

- ❑ Ref: Sasdat Malik's book

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

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

Open Issues

- ❑ Performance degradation
- ❑ Encrypted traffic
- ❑ Polymorphic attacks: change their signatures
- ❑ Human intervention: Inconvenient and slows down
- ❑ Newer and Newer Attacks: Need to keep signatures updated

Protocols for IDS

- ❑ SYSLOG Protocol
- ❑ SYSLOG Packet Format
- ❑ Remote Data Exchange Protocol (RDEP)
- ❑ BEEP
- ❑ IDMEF

SYSLOG Protocol

- ❑ RFC 3164, August 2001
- ❑ Designed for BSD. Now used on many OSs.
- ❑ Used to send event data
- ❑ Device: Originates event data
- ❑ Collector (Server): Consumes/logs/acts on event data
- ❑ Relay: forwards event data
- ❑ Sender/Receiver
- ❑ Uses UDP port 514

SYSLOG Packet Format

- ❑ 3 Parts: PRI, Header, Msg
- ❑ PRI = <nnn> = Facility*8+Severity
- ❑ Facility: 0=Kernel, 1=User-level, 2=Mail, ...
- ❑ Severity: 0=Emergency, 1=Alert, ...
- ❑ Header: Timestamp and Hostname
- ❑ MSG: Additional info
- ❑ Example:
- ❑ <34>Dec 10 22:14:15 siesta su: 'su root' failed for jain on /dev/csf/
- ❑ No connection ⇒ No security, integrity, reliability
- ❑ Reliability ⇒ Syslog over TCP, RFC 3195, November 2001

Remote Data Exchange Protocol (RDEP)

- ❑ Cisco protocol to exchange IDS events
- ❑ Alarms remain on the sensors until pulled by the management system
- ❑ Uses XML encoding for data
- ❑ Out-of-band or in-band communication using secure channel
- ❑ Ref: Joe Minieri, "RDEP Client," [http:](http://)

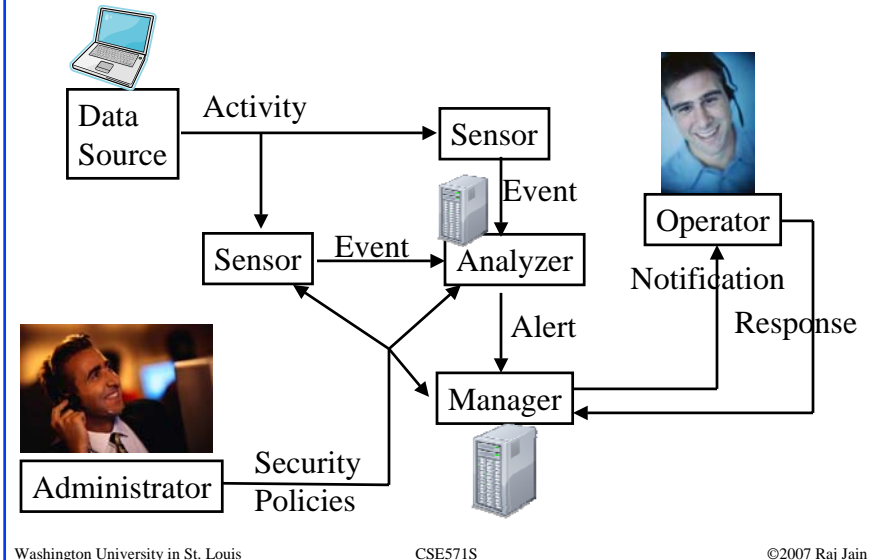
BEEP

- ❑ Block Extensible Exchange Protocol
- ❑ RFC 3080, March 2001
- ❑ Generic application protocol kernel for connection-oriented asynch interactions
- ❑ Supports both textual and binary messages
- ❑ Messages are arbitrary MIME content, usually XML
- ❑ Supports multiple simultaneous exchanges - channels
- ❑ Each channel has a associated profile that defines syntax and semantics
- ❑ Channel management profile,
- ❑ TLS transport security profile
- ❑ BEEP peer advertises the profiles it supports and later offers one of the profile for the channel

IDMEF

- ❑ Intrusion Detection Message Exchange Format
- ❑ RFC 4765, 4766, 4767, March 2007
- ❑ Many IDS sensor vendors, Many management consoles ⇒ Need standard data format and protocol
- ❑ Data format and exchange procedures for sharing IDS info
- ❑ Uses Extensible Markup Language (XML)
- ❑ Allows vendors to extend the definition

IDMEF Concepts



23-21

IDMEF Concepts (Cont)

- ❑ **Data source**: Raw network packets, audit logs, application logs
- ❑ **Sensor**: Collects from data source and forwards to analyzer
- ❑ **Analyzer**: Analyzes the data collected by sensor
- ❑ **Manager**: Used by operator to configure sensors, analyzers, data consolidation, etc.
- ❑ **Operator**: Human user of IDS manager
- ❑ **Administrator**: Human responsible for security policies
- ❑ **Activity**: Any action - Unauthorized file access, login failure
- ❑ **Alert**: Message from analyzer to manager
- ❑ **Event**: Activity that results in an alert
- ❑ **Notification**: from manager to administrator
- ❑ **Response**: Action taken in response to an event
- ❑ **Signature**: Rule used by analyzer
- ❑ **Security Policy**: Formal document on what is allowed

Washington University in St. Louis

CSE571S

©2007 Raj Jain

23-22

IDXP

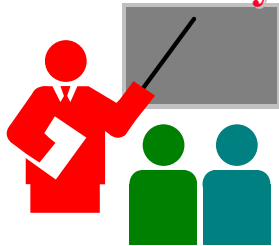
- ❑ Intrusion Detection Exchange Protocol
- ❑ RFC 4767, March 2007
- ❑ Application level protocol for exchanging IDS data
- ❑ A profile of Blocks Extensible Exchange Protocol (BEEP)
- ❑ BEEP offers the security part using TLS or Simple Authentication and Security Layer (SASL) profiles
- ❑ BEEP also has a TUNNEL profile for going over proxy servers (untrusted)
- ❑ IDXP provides the messages for IDS data exchange
- ❑ Only peer-to-peer two-party communication
- ❑ Multi-party to multi-party communication using pair-wise connections

IDMEF Example: Teardrop Attack

- ❑ Teardrop= IP Fragments with overlapping oversize payloads

```
<?xml version="1.0" encoding="UTF-8"?>
<idmef:IDMEF-Message xmlns:idmef=http://iana.org/idmef version="1.0">
  <idmef:Alert messageid="abc123456789">
    <idmef:Analyzer analyzerid="hq-dmz-analyzer01">
      <idmef:Node category="dns">
        <idmef:location>Headquarters DMZ Network</idmef:location>
        <idmef:name>analyzer01.example.com</idmef:name>
      </idmef:Node>
    </idmef:Analyzer>
    <idmef:CreateTime ntpstamp="0xbc723b45.0xef449129">
      2000-03-09T10:01:25.93464-05:00
    </idmef:CreateTime>
    <idmef:Source ident="a1b2c3d4">
      <idmef:Node ident="a1b2c3d4-001" category="dns">
        <idmef:name>badguy.example.net</idmef:name>
      </idmef:Node>
    </idmef:Source>
    ...
  </idmef:Alert>
</idmef:IDMEF-Message>
```

Summary



- ❑ Intrusion detection systems: Host based and Network Based
- ❑ Analyzers can be signature based, anomaly based
- ❑ Syslog provides a simple efficient method for IDS data
But it is not secure or reliable
- ❑ IDXP provides a secure, reliable method of IDS data exchange

References

- ❑ S. Kumar, "Survey of Current Network Intrusion Detection Techniques," http://www.cse.wustl.edu/~jain/cse571-07/p_nid.html
- ❑ NIST, Guide to Intrusion Detection and Prevention Systems (IDPS), Special Publication SP 800-94, Sep 2006, <http://csrc.nist.gov/publications/PubsSPs.html>
- ❑ Open Directory Projects IDS Page, http://www.dmos.org/Computers/Security/Intrusion_Detection_Systems/ *Has a list of 25 open source and 96 commercial tools, 79 security scanners, 25 security scanner services*
- ❑ Architectural Issues of Intrusion Detection Infrastructure in Large Enterprises, http://www.softpanorama.org/Security/intrusion_detection.shtml
- ❑ SANS Institute, "Intrusion Detection FAQ," <http://www.sans.org/resources/idfaq/index.php?portal=46489b3fa8324804cb8de1e1ff4ae9e7>

RFCs

- ❑ RFC 3080 “The Blocks Extensible Exchange Protocol Core,” March 2001
- ❑ RFC 3164 “The BSD Syslog Protocol,” August 2001.
- ❑ RFC 3195 “Reliable Delivery for syslog,” November 2001.
- ❑ RFC 4765 “The Intrusion Detection Message Exchange Format (IDMEF),” March 2007.
- ❑ RFC 4766 “Intrusion Detection Message Exchange Requirements,” March 2007.
- ❑ RFC 4767 “The Intrusion Detection Exchange Protocol (IDXP),” March 2007.

References: Books Used

- ❑ Gert DeLaet, Gert X. Schauwers, "Network Security Fundamentals," Cisco Press, Sep 2004, 400 pp., ISBN:1587051672.
- ❑ Richard Bejtlich, "The Tao Of Network Security Monitoring : Beyond Intrusion Detection," Addison-Wesley, Jul 2004, 798 pp., ISBN:321246772.
- ❑ Richard Bejtlich, "Extrusion Detection: Security Monitoring for Internal Intrusions," Addison-Wesley Professional, Nov 2005, Paperback 416 pp., ISBN:0321349962.
- ❑ Saadat Malik, "Network Security Principles and Practices," Macmillan Technical Pub, Nov 2002, 400 pp., ISBN:1587050250.
- ❑ Terry Escamilla, "Intrusion Detection : Network Security Beyond the Firewall," Wiley, Oct 1998, 348 pp., ISBN:0471290009.