

IDS & IDP

CSH5 Chapter 27

“Intrusion Detection & Intrusion Prevention Devices”

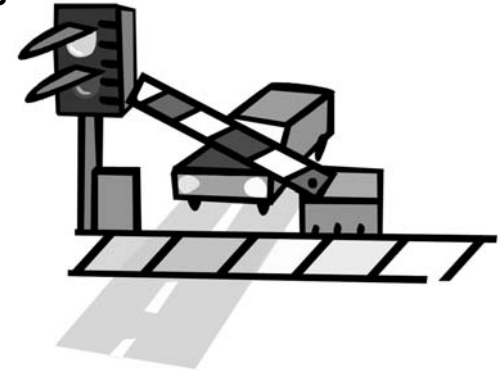
Rebecca Gurley Bace

1

Copyright © 2011 M. E. Kabay. All rights reserved.

Topics

- Security Behind the Firewall
- Main Concepts
- Intrusion Prevention
- Information Sources
- Analysis Schemes
- Response
- Needs

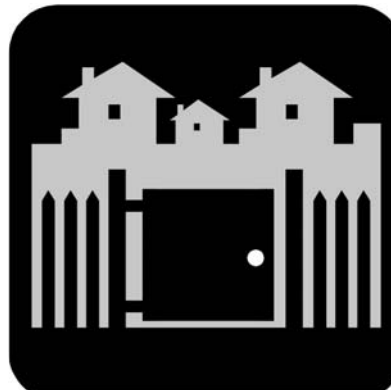


2

Copyright © 2011 M. E. Kabay. All rights reserved.

Security Behind the Firewall

- What is Intrusion Detection?
- What is Intrusion Prevention?
- Where Do ID & IP Fit in Security Management?
- Brief History of ID

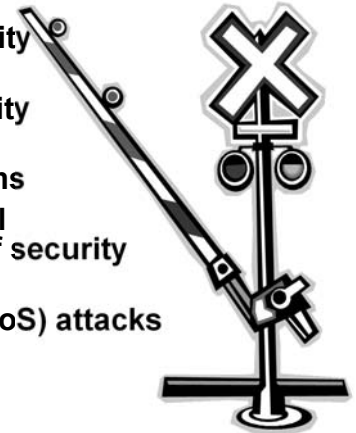


3

Copyright © 2011 M. E. Kabay. All rights reserved.

What is Intrusion Detection?

- Software or hardware
- Automate surveillance of computers and networks
- Collect & synchronize records
- Analyze data for evidence of security violations
 - ❑ Intrusions = violations of security policy
 - ❑ Attempts to compromise systems
 - ✓ E.g., attempted or successful unauthorized penetrations of security barriers
 - ✓ Includes denial-of-service (DoS) attacks

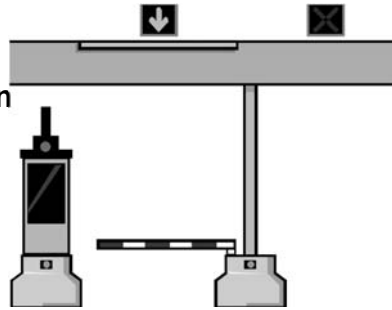


4

Copyright © 2011 M. E. Kabay. All rights reserved.

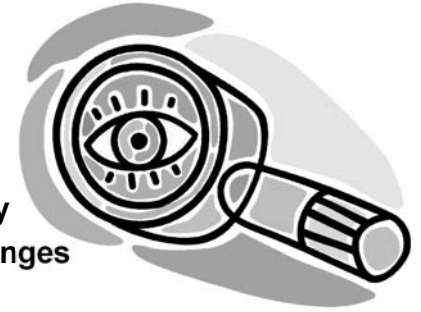
What is Intrusion Prevention?

- Coupling ID with specified responses to detected-intrusion scenarios
- Triggering events
 - Subset of intrusions
 - Better understood / characterized than generic IDS triggers
- E.g., specific traffic > specified threshold → specific response
 - Could limit traffic of that specific type
 - Time limits on response



Where Do ID & IP Fit in Security Management?

- Necessary function in system security strategies
 - ID + vulnerability assessment (VA) → *auditability*
- Auditability = ability for independent review / examine system records to
 - Determine adequacy of system controls
 - Ensure compliance with policy / procedures
 - Detect breaches in security
 - Recommend indicated changes



Audit & ID Functions

- Audit enables / supports many aspects of security management
 - Incident handling
 - System recovery
- ID
 - Flexible way to accommodate user needs
 - Retain ability to protect systems from specified threats



Will IPS Replace IDS?

- Tight coupling between IPS & audit
 - Need audit for root-cause analysis
 - Measure effectiveness of security measures
 - ✓ ID on outside & inside of firewalls
 - ✓ Justify budgets by demonstrating scope of threats, reduction inside firewall
 - Dead-chicken vs flying elephants* analogy
- But IDS & IPS insufficient
 - Also need VA, policy, controls, gateway security, I&A, access controls, encryption, file integrity checking, physical security



Brief History of ID (1)

- ID = automation of system/security audits carried out manually from earliest days of computing in 1950s
- Auditability defined as essential in 1973 paper by J. P. Anderson for USAF
- Anderson (1980) proposed automated review of security audit trails
- Dorothy Denning & Peter G. Neumann studied ID from 1984-1986 w/ report in 1986



Copyright © 2011 M. E. Kabay. All rights reserved.

Brief History of ID (2)

- Intrusion Detection Expert System (IDES, 1990)
 - ❑ Prototype instantiation of Denning's model
 - ❑ Developed at Stanford Research Institute (SRI) International
 - ❑ Hybrid system:
 - ✓ Statistical profiles of user behaviors
 - ✓ Derived from OS kernel audit logs
 - ✓ Plus other system data sources
 - ✓ Rule-based expert system
 - Configurable by users
 - Specified patterns to be flagged



Copyright © 2011 M. E. Kabay. All rights reserved.

Brief History of ID (3)

- By 1994, flurry of developments
 - ❑ Next Generation IDES (NIDES)
 - ❑ Haystack (Haystack Labs & USAF)
 - ❑ NADIR (Los Alamos*)
 - ❑ Wisdom & Sense (Los Alamos & Oak Ridge*)
 - ❑ ISOA (PRC, Inc)
 - ❑ TIM (DEC)
 - ❑ ComputerWatch (AT&T)
 - ❑ Discovery (TRW)



U.S. AIR FORCE

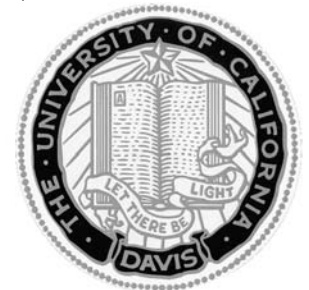


* National Laboratories of the Department of Energy (DoE)

Copyright © 2011 M. E. Kabay. All rights reserved.

Brief History of ID (4)

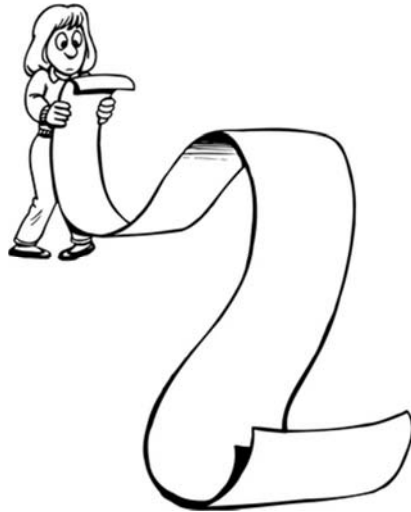
- Network-based IDS
 - ❑ Late 1980s
 - ❑ UCAL Davis
 - ✓ Network Security Monitor, later NID
 - ✓ Similar to many of today's IDS
 - ❑ Distributed Intrusion Detection System (DIDS)
 - ✓ UCAL Davis, Haystack, Lawrence Livermore National Laboratory (DoE)
 - ✓ Coordinated network-based & host-based IDS
- IPS proposed as logical next step from start of IDS research



Copyright © 2011 M. E. Kabay. All rights reserved.

Main Concepts

- Process Structure
- Approach to Monitoring
- Architecture of IDS
- Frequency of Monitoring
- Strategy for Analysis



13

Copyright © 2011 M. E. Kabay. All rights reserved.

Process Structure

Monitoring and alarm-generating process:

- Information sources (AKA event generator)
 - Network
 - Host
 - Application
- Analysis Engine
 - Look for anomalies and attacks
- Response – range of possibilities
 - Reports, logs, pagers, phone calls
 - Automated disruption of attack or raising of security barriers



14

Copyright © 2011 M. E. Kabay. All rights reserved.

Approach to Monitoring

Collecting event data and conveying data to analysis engine

- Network-based
- Host-based
- Application-based



15

Copyright © 2011 M. E. Kabay. All rights reserved.

Architecture of IDS

- Store and process audit data in different / separate environment to prevent intruder from
 - Destroying data
 - Subverting data collection and monitoring
- Also reduce load on target systems to prevent performance degradation
 - CPU usage
 - Disk I/O
 - Memory usage
 - Limited-resource usage (system tables, semaphores etc.)



16

Copyright © 2011 M. E. Kabay. All rights reserved.

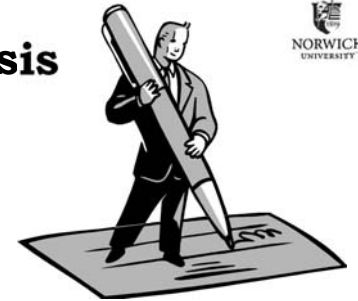
Frequency of Monitoring

- Batch-mode
 - ❑ Send data in blocks or files
 - ❑ Results *after* intrusion has started (or finished)
 - ❑ Typical of early systems due to resource limitations
- Continuous
 - ❑ AKA “real-time” data collection / analysis
 - ❑ Immediate analysis and alerts / response
 - ❑ Support intervention to reduce damage or to collect additional data (e.g., for prosecution)
 - ❑ Most common today



Strategy for Analysis

- Misuse detection
 - ❑ Filter event streams
 - ❑ Match patterns against attack signatures
- Anomaly detection
 - ❑ Statistical or AI techniques to spot *deviations* from norm
 - ❑ Definition of normal behavior becomes crucial for successful operations
 - ❑ Extremely dangerous to incorporate abnormal / unauthorized behavior into “normal” or standard data set



Intrusion Prevention

- General Concept
 - ❑ IPS often considered IDS + automated responses
 - ❑ But additional specifications have evolved
- IP System Architecture
 - ❑ Most IPS separate their functions from target (monitored) system
 - ❑ Some separate monitoring/analysis from response platform (“stand-alone”) vs “integrated” units



IP Analysis Strategy

- Strategy similar to IDS but nomenclature differs
- Rate-based analysis to block specific traffic
 - ❑ Primarily focus on network load
 - ✓ Connect rates
 - ✓ Connection counts
 - ❑ Particularly useful for detecting DDoS
- Content-based analysis
 - ❑ Anomalous packets
 - ❑ Specific content (e.g., IDS signatures)
 - ❑ Useful for malformed-packet DDoS



Information Sources for IDS

- Network Monitoring
- Operating Systems
- Applications
- Other Monitoring
- Information Source Issues



21

Copyright © 2011 M. E. Kabay. All rights reserved.

Network-Based Monitoring

- Set data-gathering station to *promiscuous mode*
 - ❑ Capture all packets going by
- Specialized devices
 - ❑ *Spanning ports* gather data from all ports on a switch
 - ❑ Specialized Ethernet network taps (sniffers) to capture network traffic



22

Copyright © 2011 M. E. Kabay. All rights reserved.

Operating Systems

- Collect data from internal sources
- Host-based monitoring can use OS data
- Often use audit-trail data (log files)



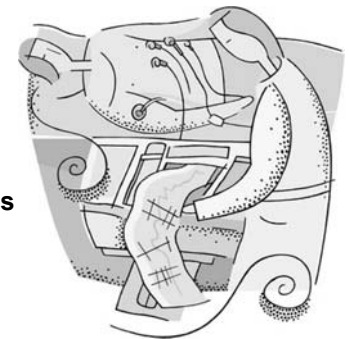
Image used with permission of Berthou.com

23

Copyright © 2011 M. E. Kabay. All rights reserved.

Application-Based IDS Monitoring

- Instrument running applications to produce data for analysis
 - ❑ Application event logs
 - ❑ Application configuration info
- Growing in importance
 - ❑ System complexity increasing
 - ❑ Object-oriented programming
 - ✓ Data objecting naming conventions
 - ✓ Make analysis of file-access logs more difficult
- *Extrusion detection* systems are special case
 - ❑ Monitor data transfers
 - ❑ Look for anomalies in movement across policy boundaries
 - ❑ Increasingly popular for compliance



24

Copyright © 2011 M. E. Kabay. All rights reserved.

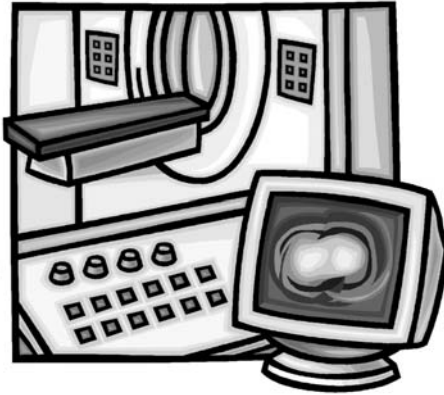
Other IDS Monitoring

- Can improve success rates of VAS by using data from other security tools

- Network firewalls
- Anti-virus software
- File-integrity checkers
- IDS

- MK adds:

- Coordination of multiple data sources leads to *cyber situational awareness (cyber SA)*



Information Source Issues for IDS

- Balance detail against performance degradation

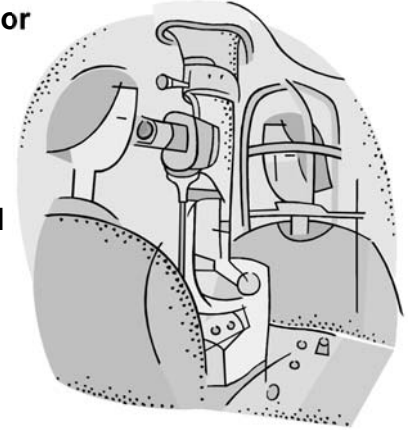
- Can overwhelm resources with data

- Monitoring appropriate areas or functions

- Chain of custody for IDS data

- Protect sensitive data in IDS data stream / collections

- Comply with legal & ethical standards



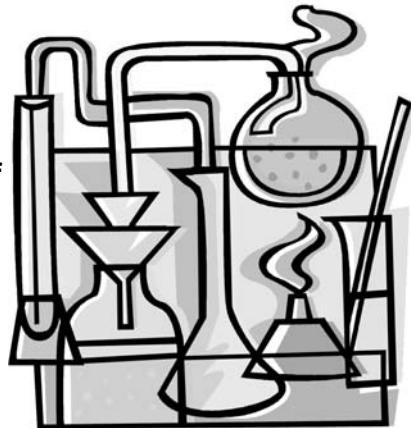
Analysis Schemes

- Analysis engine

- Accepts event data from source(s)
- Examines for symptoms of security problems

- Key issues

- Detecting Misuse
- Detecting Anomalies
- Hybrid Approaches
- Issues in Analysis



Detecting Misuse

- Filter event streams for known attack signatures

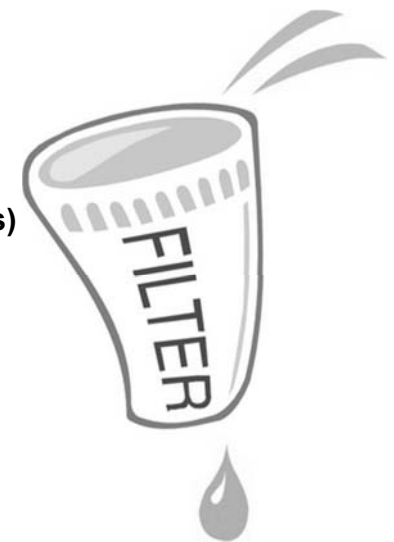
- Assumes knowledge to distinguish forbidden and authorized behaviors

- Atomic (single events) vs composite (sequences of events)

- Recognizing deviations from norm

- Complex mathematical and statistical methods

- Packet analysis – recognize malformed packets associated with attacks such as DoS and DDoS



Detecting Anomalies

- Quantitative analysis
 - ❑ Numeric rules – triggers, thresholds
- Statistical analysis – early applications to IDS
 - ❑ Calculate various statistical measures, compare to norm
- Learning (heuristic) techniques – still under development
 - ❑ Allow system to adapt to normal environment, recognize abnormal changes by itself
 - ❑ Neural networks, fuzzy logic don't usually tell security user why they identified behavior as suspicious
- Advanced techniques – R&D stage
 - ❑ Genetic algorithms
 - ❑ Data mining
 - ❑ Autonomous agents
 - ❑ Immune system



29

Copyright © 2011 M. E. Kabay. All rights reserved.



Hybrid Approaches

- Combining misuse detection with anomaly detection has been productive approach
 - ❑ Anomaly detection engine can let IDS detect new or unknown attacks or policy violations
 - ❑ Particularly useful for Internet-visible systems
 - ❑ Especially important to fight DDoS
- Misuse detection engine helpful to prevent slow modification of baseline
 - ❑ Attacker can gradually alter statistical norms
 - ❑ But misuse detector can use definitions to prevent anomaly detection engine from being subverted

30

Copyright © 2011 M. E. Kabay. All rights reserved.

Issues in ID Analysis

- Signature-based misuse detection cannot recognize new attacks
- Anomaly detection systems may have high false-positives – users turn off or ignore the alerts
- AI-based systems depend absolutely on adequate training data to distinguish *normal* from *abnormal* behavior
- Malefactors with access privileges during training can covertly teach system to accept unauthorized actions as normal



31

Copyright © 2011 M. E. Kabay. All rights reserved.

Response (1)

- Passive Responses:
 - ❑ Announce / alarm, let user handle it
 - ❑ Produce reports
- Active Responses:
 - ❑ Person-in-the-loop
 - ❑ Automated Responses
 - ✓ Collect more info about intruder / attack
 - ✓ Change environment
 - ✓ Act against intruder (hack-back) [DON'T!]
- Investigative Support – computer forensics



32

Copyright © 2011 M. E. Kabay. All rights reserved.

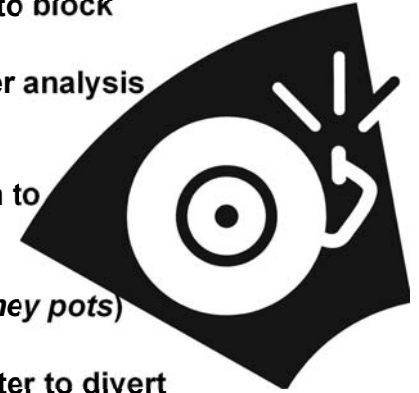
Response (2)

- Stand-alone responses
 - ❑ Use features entirely within IDS
 - ❑ Activate special rules
 - ✓ More sensitive than normal
 - ✓ More detailed
 - ❑ Thus apply focus only when appropriate & reduce false positives during normal times



Response (3)

- Integrated responses
 - ❑ Change systems settings to block attacker's actions
 - ❑ E.g., increase logging, alter analysis engine settings, check for vulnerabilities
 - ❑ Can instruct target system to fix known vulnerabilities (*immune function*)
 - ❑ Deploy decoy system (*honey pots*) to deflect attacks
 - ❑ Reconfigure switch or router to divert attacks



Problems in Responses

- Needs are highly variable
- False-positive rates must be tunable
- Automated responses can cause self-directed DoS
 - ❑ E.g., shutting off access to apparent source of attack
 - ❑ But attacker can spoof source in IP packets



Needs Assessment and Product Selection

- Matching Needs to Features
- Specific Scenarios
- Deployment of IDS



Matching Needs to Features

- Reduce incidence of problem behavior by increasing likelihood of discovery
- Detect security violations
- Documenting existing threats
- Detect and reduce attack preambles (probes, scans etc.)
- Diagnose problems (e.g., bad configurations)
- Test effects of upgrades and maintenance on security
- Provide forensic evidence of crimes



37

Copyright © 2011 M. E. Kabay. All rights reserved.

Specific Scenarios

- Establishing threat levels for new networks
- Protecting Web servers
 - Informational
 - Transactional (harder to protect)
- Monitoring specific applications or servers
 - E.g., particular databases



38

Copyright © 2011 M. E. Kabay. All rights reserved.

Deployment of IDS (1)

- Location of sensors
 - Outside main firewall
 - In DMZ
 - Behind internal firewalls
 - In critical subnets
- Scheduling integration
 - Don't rush the installation
 - Let system accumulate knowledge of normal patterns – will reduce false alarms

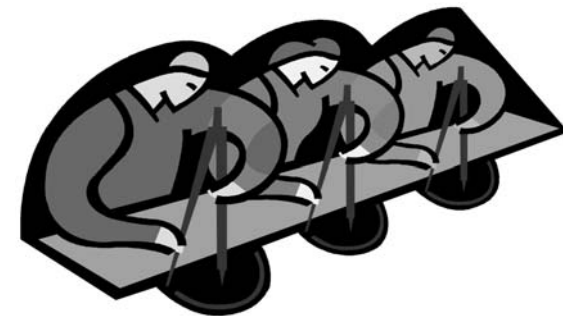


39

Copyright © 2011 M. E. Kabay. All rights reserved.

Deployment (2): Adjusting alarm settings

- May suspend alarms for weeks or months
- Allow adaptation of the IDS to monitored system
- Allow operators to learn how to work with IDS



40

Copyright © 2011 M. E. Kabay. All rights reserved.

DISCUSSION