



Intrusion Detection and Intrusion Prevention

E. Eugene Schultz, Ph.D., CISSP, CISM
University of California-Berkeley Lab
eeschultz@lbl.gov

ISACA-San Francisco
October 5, 2004



Agenda

- Introduction
- Recent advances in intrusion detection
- IDSs versus IPSs
- Achieving ROI with IDSs
- Conclusion



About intrusion detection

- Definition: the process of discovering unauthorized use of computers and networks
- Is really misnamed---should really be called “attack detection”
- Intrusion detection systems (IDSs) automate the discovery process



Types of data that can be used

- Firewall data (this is the best source, all things considered)
- Audit log data from systems
- Data from passive devices (e.g., sniffers)
- Data from packet filters (e.g., TCP wrappers)
- Data from integrity checking tools (e.g., Tripwire)
- Output of intrusion detection systems (IDSs)
- Others

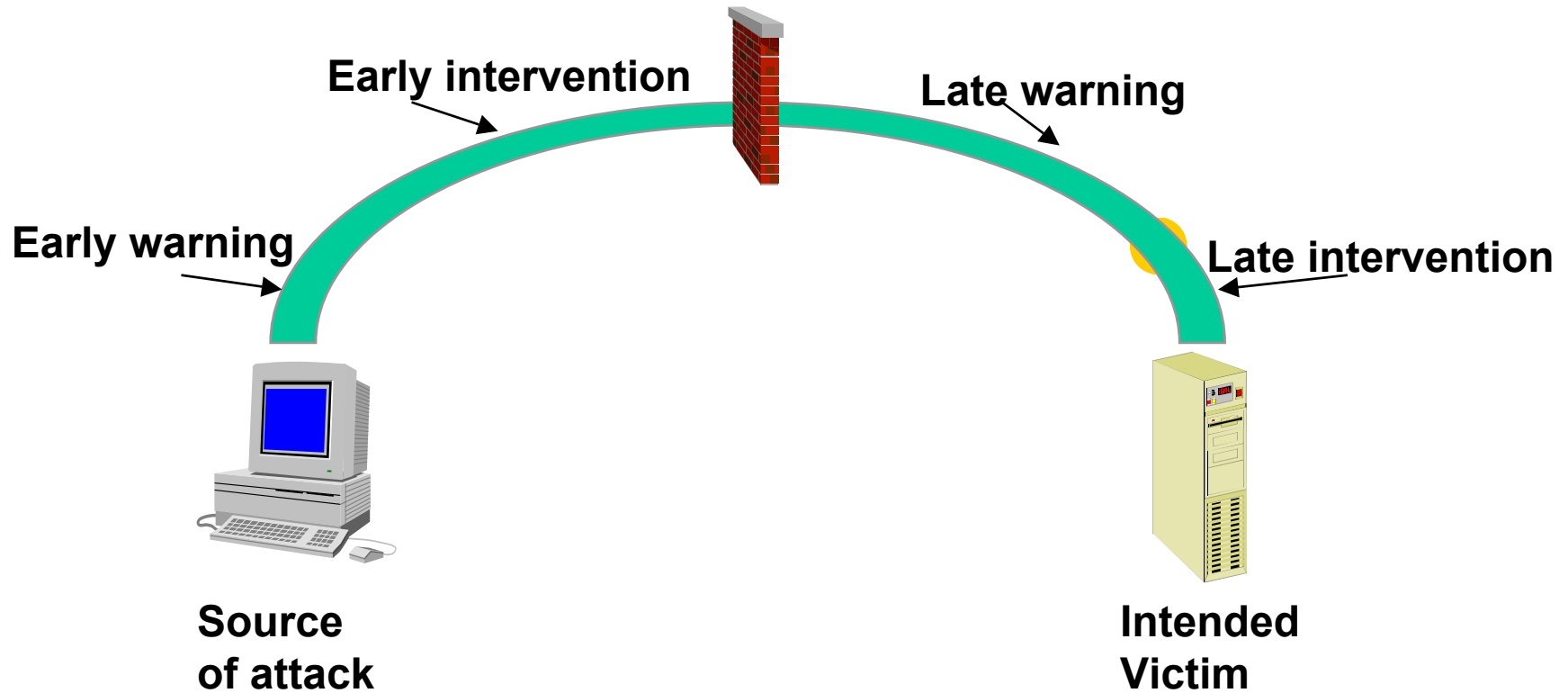


What should be the focus of intrusion detection capability?

- Points of network traffic entry
- Critical servers
 - Business application servers
 - Web servers
 - DNS servers
 - Critical database servers
- Network zones with higher security needs



How intrusion detection is related to ability to intervene





Types of IDSs

- Anomaly detection systems
 - Designed to discover anomalous behavior
 - Look for unusual usage patterns by users
 - Often based on statistical profiles (e.g., time, amount and type of usage)
- Misuse detection systems
 - Focus on symptoms of misuse by *authorized users*
 - Examples: unauthorized logons, failed logon attempts, attempts to mount file systems of sensitive systems



Types of IDSs

- Target monitoring systems
 - Report whether certain target objects have been changed
 - Usually work through a cryptographic algorithm to compute a cryptochecksum for each target file
 - The IDS reports any changes in crypto checksums
 - Examples: logon programs, dynamic link libraries (DLLs)
 - Many advantages over other approaches (e.g., you do not have to continuously monitor)
- Systems that perform wide-area correlation of slow and stealth probes
 - Slow and stealth probes can evade normal IDSs
 - Perform wide-area collection and correlation of slow and stealth probes

Continued



Reasons to utilize IDSs

- Greater proficiency (as opposed to humans) in detecting intrusions
- Can provide technical expertise not otherwise available
- Can provide a wealth of information useful in dealing with an attack
- Reduction of manpower needed to discover incidents
- Capability of dealing with large volumes of data



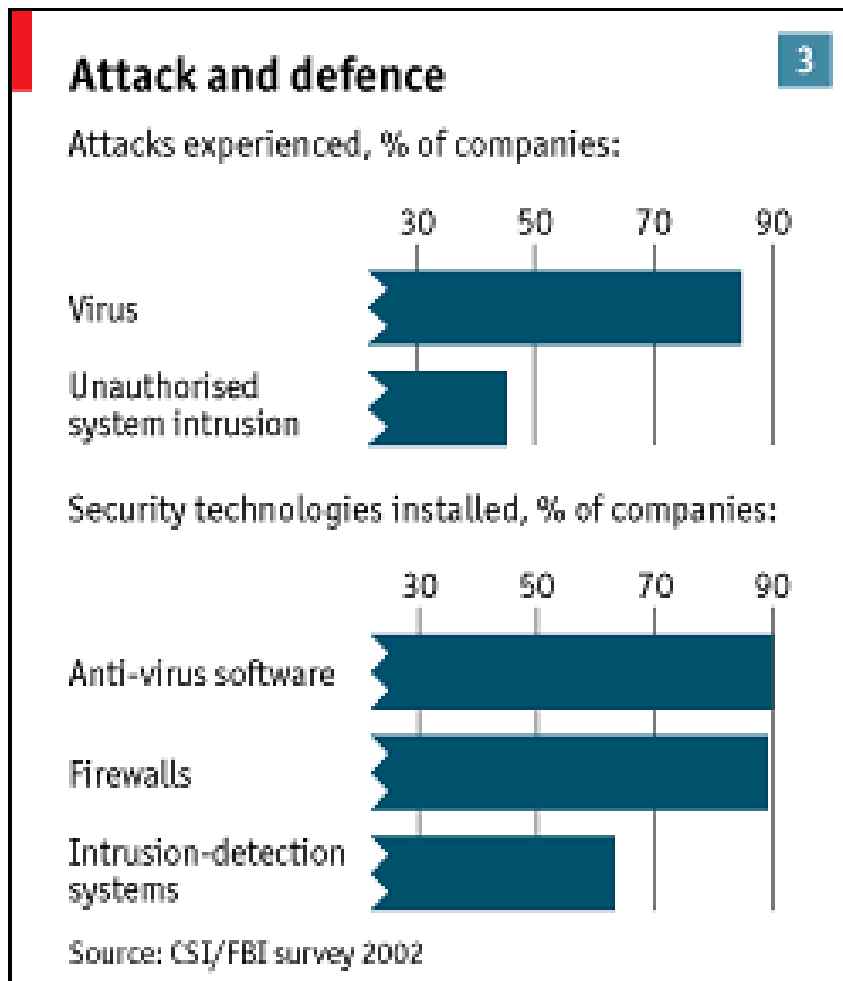
Reasons to utilize IDSs

- Can reduce damages and potential damages because of near real time alerting capabilities
- Can provide automated responses
 - Logging off a user
 - Disabling a user account
 - Launching of scripts
 - “Shunning” (blocking) IP addresses
- Deterrent value
- Built-in forensics capability (in several)
- Built-in reporting capability (more and more)

Continued



Intrusion detection systems are used by two-thirds of organizations surveyed





Agenda

- Introduction
- Types of intrusion detection
- IDSs versus IPSs
- Achieving ROI with IDSs
- Conclusion



Types of intrusion detection

- Network based---a host looks at network traffic (and also possibly fuses information sent from hosts)
- Host based---software resides on individual systems



Network-based intrusion detection



→ Alarm!

IDS

```
net use * \\128.8.45.139\C$
```



Source
of attack



Intended
Victim



Rationale for network-based intrusion detection

- Has a broader scope than host-based intrusion detection
- The majority of attacks that occur now originate from *outside* one's own organization
- Can fuse multiple sources of data
- Not dependent on system audit data
- Can be effective even when multiple hosts within a network are compromised



Rationale for network-based intrusion detection

- Is generally easier to set up
- More cost-effective (usually)



Continued



Examples of network-based intrusion detection tools

- Snort (runs on Unix, Linux, Windows)
- RealSecure (Unix, Linux, Windows)
- Symantec Intrusion Detection (Unix, Linux))
- Dragon (Unix and Linux)
- Network Flight Recorder (NFR) (Unix, Linux, Windows)



Limitations of network-based intrusion detection

- Considerations related to network throughput
 - Any rate much greater than 300 - 400 Mb/sec starts to become a problem with network-based IDSs
 - Getting top-performance hardware on systems that house network-based IDSs helps very little
 - Sensors tend to work fairly slowly
 - Network detection rate and processing speed will probably always lag behind the actual rate of traffic flow
- Packet loss can have huge consequences
- Packet fragmentation causes complications
- What if an insider gets loose within a network?



Limitations of network-based intrusion detection

- Susceptible to “slow and gradual” attacks
- Cannot deal with encrypted network traffic
- Others

Continued



Host-based intrusion detection

- Key--each host obtains data that could signal the presence of an attack
 - Audit data
 - Changes in files or directories
 - Output of commands such as netstat

Active Connections

Proto	Local Address	Foreign Address	State
TCP	198.128.4.231:2178	128.3.41.19:143	ESTABLISHED
TCP	198.128.4.231:2180	128.3.41.19:143	ESTABLISHED
UDP	198.128.4.231:137	*:*	



Host-based intrusion detection

- Better-suited to discovering insider attacks than is network-based intrusion detection
- Data aggregation by a central host can greatly improve the capability of host-based intrusion detection

Continued



Limitations of host-based intrusion detection

- In and of itself, host-based intrusion detection is based only on whatever any single host can record
- Is less conducive to early intervention than network-based intrusion detection
- Audit logs and other data produced by systems can be tampered with
- Can get expensive very quickly





Examples of host-based intrusion detection tools

- Tripwire (freeware version) (runs on Unix and Linux)
- Tripwire (commercial version) (Unix, Linux and Windows)
- TCP wrappers (Unix and Linux)
- Psionix Port Sentry (Linux)
- Dragon (Unix and Linux)
- CMDS (Unix and Linux)



Agenda

- Introduction
- Recent advances in intrusion detection
- IDSs versus IPSs
- Achieving ROI with IDSs
- Conclusion



Recent advances in intrusion detection*

- Substantially better ability to keep up with network throughput rates
- Less reliance on attack signatures
- Increasing ability to perform event correlation
- Better reporting capabilities
- Forensics and data archiving capabilities

* - At least in some leading intrusion detection systems (IDSs)



Implications for commercial sector

- These advances have increased the benefit to cost ratio for organizations considerably
- BUT--the Gartner Group has predicted the rapid demise of intrusion detection technology



Agenda

- Introduction
- Recent changes in intrusion detection
- **IDSs versus IPSs**
- Achieving ROI with IDSs
- Conclusion



Pros of intrusion detection

- Provides a reality check of the security of systems and networks
- Different IDS options (e.g., host- versus network-based intrusion detection) can fill different business needs
- Price is becoming less of a consideration (although some solutions are still mega-expensive)
- Can greatly reduce manpower needed in diagnosing attacks
- Can deter attacks
- Is considered part of due diligence



Cons of intrusion detection



- Lags exist between the time events occur and the time they are detected
- “Zero day attacks” are a significant problem for most intrusion systems
- Most IDSs cannot keep up with high throughput rates
- Intrusion detection evasion techniques have proliferated
- Intrusion detection systems are vulnerable to attack
- False positive rates for many intrusion detection systems are unacceptably high
- Critics say that intrusion detection does not go far enough



About “shunning” in IDSs

- Many IDSs can dynamically block subsequent traffic from originating (source) IP addresses associated with attacks
- Is thus actually a form of intrusion prevention
- Although potentially good for security, shunning has some distinct limitations
 - Source IP address spoofing is widespread
 - Blocking traffic for certain IP addresses is at best a transitory solution
 - Shunning mechanisms themselves are usually less than perfect
 - Legal problems may surface



About intrusion prevention

- Resource requests to a system initiated by applications are
 - Evaluated in real-time
 - Granted or rejected according to the particular application security policy in use
- Stops
 - Potentially dangerous file system manipulation requests
 - Attempts to overrun input into memory
 - Potentially dangerous network commands
 - Abnormal application states
 - Bypassing of security operations
 - Other negative outcomes



Case study: ImmuneEngine*

- Clients reside on each host
 - Each looks for unauthorized activities (suspicious program installations, change in file locations, etc.)
 - Creates a dynamic map of areas that need to be protected on each host and then uses it to develop a protection matrix
 - Scans for unauthorized changes
 - If an unauthorized event happens, ImmuneEngine stops it from going any farther and reverses any changes that occur
- The server
 - Receives reports from clients
 - Provides central monitoring

* - Visit http://www.bbstechnologies.com/prod_immune_engine.html



Pros of intrusion prevention

- Can actually ward off the effects of attacks
- “Zero day” attacks are not nearly as much of a problem as with IDSs
- Not reliant upon attack signatures
- Fairly easy to run and maintain
- Small impact upon system and network performance (generally)



Cons of intrusion prevention

- Heavily reliant on changes in systems--but there are so many changes
- False alarms can be catastrophic
- Technology is still rather crude
- Economic cost is generally high





So was the Gartner Group right?

- Probably not
 - The IDS market has expanded substantially since Gartner's prediction
 - Right now intrusion prevention is more “hype” than substance
 - Intrusion detection and intrusion prevention are not necessarily orthogonal to each other
 - Defense in depth is the best approach to information security, anyway



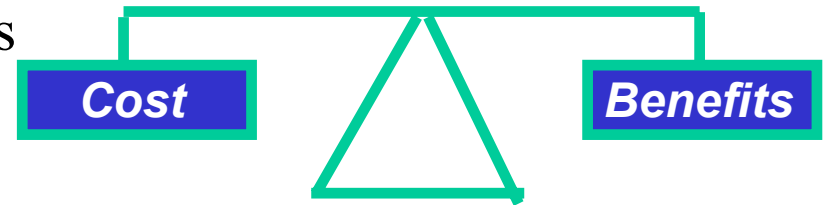
Agenda

- Introduction
- Recent changes in intrusion detection
- IDSs versus IPSs
- Achieving ROI with IDSs
- Conclusion



Achieving return on investment (ROI)

- Key--quantitizing what intrusion detection provides
- Some key metrics include
 - Reduction of expected loss due to security breaches
 - Containment of loss when security breaches occur
 - Reduction of misuse
 - Containment of personnel costs
 - Prevention of down time
 - Better quality of service
 - Reducing legal liability
- *Failure to establish ROI is currently one of the biggest problems with intrusion detection!*





Developing an intrusion detection architecture

- An “architecture” includes
 - A high-level characterization of how different components within a security practice are organized
 - How the components relate to each focus within that practice
- Start at the highest level, ensuring that policies include appropriate provisions for deploying, managing, and accessing intrusion detection technology
 - Access to IDS output (particularly sniffed data)
 - How data are captured and archived
 - What to do when an attack is detected



Developing an intrusion detection architecture

- Write specific standards appropriate to each type of IDS deployed
 - Minimum hardware configuration needed
 - Upgrading of signature libraries
 - Minimum disk space that needs to be available
- Develop appropriate guidelines and recommendations
- Be sure to remember the “people element” in your intrusion detection architecture
 - Having the appropriate technical skills
 - Training
 - Personnel policies

(Continued)



Protecting systems and sensors used in intrusion detection

- Ensure that each system and sensor that yields or processes intrusion detection/prevention data is
 - Up-to-date with patches
 - Configured in a secure manner
- If possible, set up redundant systems for all critical systems
- Use the “least privilege principle” concerning administration of systems used for intrusion detection/prevention
- Ensure that remote access methods are secure (but if possible, do not allow any remote access)



Interfacing with the incident response component

- There should be one or more humans in the loop on a 24 X 7 basis
- Critical tasks
 - Documenting all relevant data and occurrences
 - Separating the “wheat from the chaff”
 - Gauging the size and impact of each incident
 - Establishing priorities and following them
 - Dealing with forensics considerations right from the start of each incident
 - Doing what is necessary to preserve the integrity and availability of systems used in intrusion detection



Agenda

- Introduction
- Recent changes in intrusion detection
- IDSs versus IPSs
- Achieving ROI with IDSs
- Conclusion



Conclusion

- Intrusion detection has moved from an obscure to a mainstream activity in organizations
- It is important to keep up with changes in intrusion detection capabilities---big ones are constantly occurring
- Be wary of the “hype” (and snake oil) surrounding intrusion prevention systems
- Achieving ROI in information security is difficult--achieving ROI in intrusion detection/prevention is no exception



Conclusion

- There is a big difference between having intrusion detection/prevention technology and making this technology meet business needs
- Necessary ingredients for making intrusion detection technology work in your organization include
 - Time
 - Proper planning and implementation
 - Resources
- Suggestion: if you are not already doing so, start deploying some kind of intrusion detection/prevention technology soon

(Continued)