

A Justification for Intrusion Detection

by Linda McCarthy

Executive Security Advisor
Office of the CTO

INSIDE INSIDE

- > Why invest in intrusion detection systems?
- > Types of intrusion detection systems
- > Cost of expansion

Contents

Introduction3

Why invest in intrusion detection systems?3

Types of intrusion detection systems4

 Network-based4

 Host-based4

 Decoys5

 Signature-based detection5

 Protocol-anomaly detection6

 Protocol-based vs. signature-based systems6

Cost of expansion7

Appendix A: Symantec™ ManHunt and Symantec™ Decoy Server8

About the Author12

> Introduction

Corporate networks do not become safe simply because someone installs a firewall. Network security begins before the systems ever come out of the box. The organization must understand how to install them securely before they are connected to the corporate network. Installation procedures and security priorities are set by a corporate policy. Such policies fall under an organization's information-protection program and are driven by corporate goals and the culture of the company. Security policies protect the corporation's information from unethical activity such as the theft of trade secrets by an unauthorized individual.

A compliance program needs to include monitoring to know when system and network policies are abused. Without monitoring in place, executives will never know if their security policies are enforced.

Corporations have good business and legal reasons for setting up suitable policies and an adequate compliance plan. Like the existence of strong, clear policies themselves, monitoring for abuse of policy is a foundation of security. A corporation that fails to monitor for policy abuse is missing an important component of security. Thus, intrusion detection software must be installed on a network, because it monitors for abuse of policy. If a corporation has not invested in intrusion detection software, it needs to. Holding off on this investment puts the corporation at risk not only from modification, destruction, and theft of data, but also of legal action if something bad happens and lawyers get involved. One question that was asked in a recent court case involving a credit card company was, "Did you have security policies and monitoring in place?"

Because intrusion detection is critical to monitoring compliance with every network security policy, this document discusses intrusion detection and some considerations that justify it and help improve business.

> Why invest in intrusion detection systems?

An intrusion detection system (IDS) monitors and analyzes events that occur on a network or system, looking for intrusion attempts (events that try to compromise the confidentiality, integrity, and availability of data).

The increase and severity of attacks now make intrusion detection systems a necessary part of security. Since most networks require intrusion detection, a corporation must understand what type of IDS provides the functions needed to protect its infrastructure. Corporations sometimes invest in an IDS that is difficult to support, reports far too many false positives, and cannot keep up with the speed of the network.

False positives are seeming attacks generated by legitimate activity. A system administrator may believe that an attack took place when in fact none ever occurred. An IDS that reports many false positives is difficult and often impossible to manage. After a while the system administrator may ignore alerts because they look like false positives, or the administrator stops looking at the alerts and data being collected because it is too difficult to figure out if an attack actually took place.

If the corporation is not looking for intrusion attempts it has no idea what the threat to the organization is. Once in place, an IDS will report threats that can substantiate claims that the network is under attack. Understanding the frequency and types of attacks allows an organization to determine what security controls need to be in place. IDSs simplify the task of verifying and categorizing the threat in reports to executive management. This solid information helps sell management on budgeting for additional security. For example, if you put only one sensor at the gate of your network and can show management how often you are attacked, how severe the attacks were, and how you were warned of zero-day attacks such as Code Red, then management will most likely understand the need to monitor other important areas on the network, like partner connections and virtual private networks.

> **Types of intrusion detection systems**

NETWORK-BASED

Network-based IDSs capture and analyze packets that pass on the network segment by placing the network interface card in promiscuous mode. Each sensor looks only at packets that are carried on the network segment to which the sensor is connected, thus protecting multiple hosts connected to that segment. A sensor can also be on a boundary device such as a switch allowing it to inspect all packets on the subnet. A network deployment typically consists of one or more sensors performing local analysis and reporting attack information back to a centralized console.

HOST-BASED

Software needs to be loaded directly on the host to be monitored. Once deployed on the host, the software monitors system files, processes, and log files for suspicious activity. In addition, some host-based IDSs can monitor for changes in user privileges. Gaining higher-level privileges or setting up new user accounts is a common approach used by an adversary on the internal network. On critical servers, detection of this kind of abuse is important and needs to be monitored directly on the host. Therefore, experts recommend a combination of host-based and network-based detection on large networks. Understanding the high-risk areas on the network is key to a successful deployment for both network-based and host-based intrusion detection.

DECOYS

A decoy (sometimes referred to as a “honey pot”) is a system that, when installed on a critical network, is designed to lure a potential hacker away from other more important systems on that network. Diverted from critical information, the attacker grabs the bait, and the system administrator is warned of unauthorized activity in this zone. Decoys are placed throughout corporations and financial institutions in conjunction with network-based and host-based IDSs. The decoy’s ability to pick up slow scans (when other IDSs cannot) makes it a complementary solution.

Decoys involve designing a system considered to be of interest to a potential attacker. The system needs to look real, have real data, and have enticing enough data to keep the attacker around while you capture his moves. You can learn much about the skill of the attacker once captured. Is this just someone playing around? Does he really know his stuff? Ideally, once the attacker is in the decoy, tracking him or her back to the real source of the attack, and then watching and recording (digitally stamping) every keystroke, prepares you with evidence to capture the attacker and take legal action.

Firms should not rely on statistics alone to understand their internal threats. Internal networks are hostile. The insider is the most dangerous because he or she knows the security policies and weaknesses. Relying on statistics to understand the gravity of this threat is risky. By contrast, placing decoys throughout a firm can produce evidence that helps executive management understand the threat of unauthorized use by insiders. Proof of abuse detected through these systems can help fund additional security initiatives.

SIGNATURE-BASED DETECTION

A majority of IDS products are signature-based; they examine the network packets traffic for specific patterns of attack. Signatures must be developed specifically for the attack so the IDS can recognize the attack. These systems require large signature databases so that every packet can be compared to the database. One of the greatest challenges of these systems is they must have advance knowledge of the attack to be detected. Because new attacks are discovered every day, intrusion detection systems relying solely on this approach will always be out of date.

The other challenge for these systems is keeping up with the speed of the network. As network speeds increase, the sensors lack the resources to look at every packet, so some packets are discarded. Attacks could easily go unnoticed by the IDS. In addition, higher speeds can increase the false positive rate. Higher-speed networks are resulting in decreased detection and increased false positives.

PROTOCOL-ANOMALY DETECTION

Protocol-anomaly detection focuses on the content of the network communications at the protocol level. Many attacks target protocols such as Telnet, HTTP, RPC, and SMTP. Packets are statefully inspected in the context of previous packets of the same conversation. As a conversation progresses, it is evaluated by a protocol state machine to determine if the protocol has been abused in any way. The state machines, which cover the popular protocols in layers three through seven, are derived from the RFC protocol standards. Common misuses of the protocols are also built into the state machines to allow for legitimate network traffic that deviates from the protocol standards. Attackers can use certain programming errors (buffer overflows) to compromise or damage a system. These attacks exploit poor programming practices and are quite common. When protocol rules are modeled directly in the sensors, it is easy to identify traffic that violates the rules, such as unexpected data, extra characters, and invalid characters.

PROTOCOL-BASED VS. SIGNATURE-BASED SYSTEMS

Protocol anomaly detection eliminates the need for extensive attack-signature databases, which have plagued legacy IDSs with scalability and manageability issues. More important, watching for protocol anomalies is a more effective method of attack detection than watching for attack signatures. New attack methods and exploits are constantly being discovered. By contrast, new protocols and extensions to existing protocols are developed more slowly. The rules to ensure that a conversation is adhering to the protocol standards are specified in the protocol RFCs. Any deviations from these rules create protocol anomalies.

Given the types of attacks to date, experience shows that 80% of attacks violate protocol rules. Hackers develop programs that attack poorly defined areas of protocol; attacks can be spotted by protocol-anomaly-based IDSs. Protocol-anomaly IDSs detected Code Red attacks, unlike signature-based systems, which had to wait for an update to detect the attacks while leaving the firm at risk. The protocol-detection module is a precise model of the HTTP protocol based on its RFC. The Code Red attack violates the HTTP protocol because it uses a GET request to post and execute malicious code on the victim server. Protocol IDSs recognize the violation and alert the administrator that an attack just occurred.

A firm must know the moment it is under attack. Between the launch of a new attack and the time when the security community becomes aware of it (and develops countermeasures), an adversary can take advantage of that window of opportunity to penetrate existing defenses. Threats at this point in their life cycle are called zero-day attacks. Because they are not publicly known, they are not yet reflected in detection signatures and can sidestep existing defenses. This is a powerful reason for a firm to deploy protocol detection. Signature-based systems must wait for an update before they become able to detect the new attacks.

Moreover, that signature will protect only against that specific attack. Signatures are very specific to an attack. After a particular attack, a slight modification to the detected attack can enable the new variant to make its way past the intrusion detection system. This well-known strategy allows hackers to subvert signature-based intrusion detection systems.

When a signature-based system is updated with a new Code Red signature, for example, the firm will be protected only until the next variant is released. The first signature created for detecting Code Red attacks contained a simple string of characters. The string was a characteristic of the initial Code Red attack but not its basis. Code Red II soon followed. While it violated the HTTP protocol in the same manner as Code Red, signature-based IDSs could not detect the Code Red II attack since it contained a variation of the string.

Useful though they are, signature-based systems alone cannot provide early warning against zero-day attacks such as Code Red. Because some attacks do not violate protocols, it is helpful to use signature-based systems in conjunction with protocol anomaly, deploying a layered approach to detecting attacks.

> **Cost of expansion**

The costs of first deploying signature-based and network-based intrusion detection systems are similar. What most corporations miss, however, is that IDSs designed for high-speed switched networks cost less to expand than do traditional systems.

A traditional signature-based deployment, based on the number of sensors deployed, requires one sensor for each network segment, plus the cost of hardware, software, and systems administration. When the corporation needs to expand deployment for full network coverage, the costs associated with funding sensors, hardware, software, and system administration will be comparable to the costs of those components in the initial installation. A company that wants to monitor 10 more segments of 100 megabits each, for example, will pay for 10 more systems and software, 10 sensors, a management console, and systems administration costs to support those additional systems.

Some IDSs designed to work on high-speed switched networks, however, allow for maximum coverage without the added cost of system administration. Connecting at the switch keeps the system from being restricted to monitoring one segment, and a single node can monitor a Gigabit of traffic. If the IDS has a roaming feature, it can provide larger network coverage. With roaming enabled, an IDS can be compared to a set of security cameras in convenience stores. One camera may always monitor the front door and the cash register. Other cameras take snapshots of the front and back parking lots. Thus they capture enough evidence for police to review if an incident occurs. Unlike security cameras, the IDS should have the intelligence to know that an incident occurred at the backdoor, to continue collecting data, and to alert the system administrator. With this type of IDS, a corporation's savings on support, deployment, and maintenance alone can be large.

> **Appendix A: Symantec™ ManHunt and Symantec™ Decoy Server**

SYMANTEC MANHUNT

Symantec ManHunt is a threat management solution that enables a company to maintain control and respond to intrusions and denial of service attacks for the enterprise network. Symantec ManHunt provides a highly coordinated approach to managing security issues, from identifying threats on the network and gathering additional information on demand, to responding quickly and taking appropriate action.

Detection

Symantec ManHunt sets a new standard in attack detection with high-speed traffic monitoring up to 2 Gigabit per second, allowing implementation at virtually any level within an organization, even Gigabit Ethernet. Through the use of distributed sensors, Symantec ManHunt provides hybrid threat detection that can identify previously unknown and new attacks as they occur. The hybrid detection architecture provides flexible solutions to customize sensor detection capabilities to the surrounding environment. Using an array of detection methodologies to enhance attack identification, Symantec ManHunt collects additional evidence of malicious activity by traffic behavioral monitoring, protocol state tracking and IP packet reassembly. This capability, dubbed “zero-day” detection closes the window of vulnerability inherent in traditional IDS systems that leave other networks exposed.

Analysis

The analysis and correlation engine of Symantec ManHunt successfully makes sense of the numerous events taking place on the network, and evaluates them in context. Time and knowledge are critical in order to mount an effective and rapid response to attacks on mission critical enterprise assets as they occur. Real time event aggregation, correlation and analysis enables Symantec ManHunt to collect events from security devices throughout the enterprise and uses advanced event correlation and analysis to quickly recognize events as they happen. This dramatically reduces the effort traditionally required by security personnel, giving them time for more sophisticated intrusion investigation and policy work instead of spending hours examining uncorrelated event logs.

Collecting events from third party security sources enables Symantec ManHunt to extend the threat management umbrella beyond events collected from hosts to cover the entire enterprise. Snort (open source IDS), Host IDS, Tripwire, Okena (now Cisco) StormWatch, and Netscreen in the host IDS space.

Response

Symantec ManHunt goes a step beyond simple notification by providing automated policy-based responses to protect systems and buy time and peace of mind for security personnel.

When it is desirable to locate the source of an attack, most often with a spoofed address, the traditional approach is to manually interrogate routers, hunting for the relevant stream of data. This is a grueling exercise that can take many hours to many days, even for a skilled network engineer. Using FlowChaser technology with TrackBack, Symantec ManHunt can quickly and automatically trace attacks, even those that are spoofed or reflected, back to the ingress point of a network. This allows enterprises to react quickly and efficiently to block denial-of-service attacks that can seriously impact bandwidth and service availability. In addition, features such as policy-based response, payload inspection and CVE support provide security personnel with enough information to discover even the subtlest attacks.

Deployment

With the ability to deploy cooperative clusters across the enterprise and built-in attack hardening, Symantec ManHunt handles the largest and most demanding deployment scenarios. Unlike traditional intrusion detection sensors, it gathers its primary detection data directly from switches through copy ports, decreasing the number of sensors needed to be deployed, managed and maintained, lowering the Total Cost of Ownership (TCO).

SYMANTEC DECOY SERVER

Symantec Decoy Server is the industry-leading Deception-based Intrusion Detection System (DIDS) that minimizes the risk of compromise through advanced detection and response mechanisms found solely in deception based security solutions. Deception as a means of defense provides a solution that enables real-time attack detection in a dynamically changing environment, while at the same time, lowers the overhead of threat management by eliminating false positives and uncovering the severity of threats directed towards the infrastructure.

Detection

Symantec Decoy Server has the unique ability to detect threats by becoming the target of the attack. When attacks are directed at the sensor, it delivers holistic attack detection through a system of data collection modules. Every action of the attack is recorded for live attack analysis, allowing the organization to categorize the extent of the threat and take appropriate responses. Since the software is not time or signature limited, novel attacks are detected and responses are taken. By staying at the forefront of an attack lifecycle, the organization can fortify the rest of the network against further instances of attack. Early warning sensors such as Symantec Decoy Server have proven value by giving the organization the information that is so crucial to maintaining a productive network infrastructure.

Analysis

Symantec Decoy Server maintains an audit trail of the attacker's activities, and logs relevant activity in the cage, such as keystrokes, process invocation, and file accesses. The alerting system can be configured to send alert messages based on specific classes of events. The software has an extremely low rate of false-positives, since any traffic directed at the Symantec Decoy Server cage is considered suspicious.

Deployment

Symantec Decoy Server cages can be easily configured to resemble currently existing hosts within a network or they may be configured to look slightly more vulnerable than the surrounding servers and can be an effective way to lure attackers. Symantec Decoy Server has the unique quality of a “set and forget” intrusion detection system. Upon deployment, the management staff will only have to attend to the systems during instances of attack. There are no signature updates or policy configurations. A lower management requirement permits the security staff to concentrate on defending the enterprise rather than focusing on the software generating (sometimes false) threats.

Symantec Decoy Server hosts may also be configured to reside in a multitude of ways within a DMZ to provide an integral security component against external attackers. As with internal attacks, a Symantec Decoy Server cage can be configured to resemble another host, like a public FTP, mail or web server. To combat attackers who have access to the network from inside, Symantec Decoy Server hosts can be placed in strategic locations throughout the network.

> **IDS Network Evaluation Template***

DETECTION

- Protocol anomaly detection
- DoS attack detection
- Network infrastructure attack detection
- Common application protocol detection
- Stateful signature detection
- Custom signature support
- Full protocol decode
- Evasion detection and resistance to IDS attack
- Full fragment reassembly
- Full multi-interface reassembly

ANALYSIS

- Third-party event integration
- Real-time event aggregation
- Real-time analysis
- Automated correlation and prioritization
- Cross-node event correlation
- Full packet capture
- Secure data store
- Duplicate suppression
- User tunable controls

RESPONSE

- Automated policy-based response
- Alerting (SNMP, email, console log)
- Session termination
- User-defined response actions
- Traffic recording and playback
- Remote threat tracing
- Peer network event notification
- Session blocking suggestions or integration

PERFORMANCE/SCALABILITY

- Full 100 Mbps throughput (no packet loss)
- Full 1 Gbps throughput (no packet loss)
- Multiple 100 Mbps segment throughput (no packet loss)

- Handle 500,000 simultaneous TCP sessions
- Scales to 100s of sensors
- Robust under edge conditions

MANAGEMENT

- Secure remote management
- Broad platform support for management
- Scalable information presentation
- Incident drilldown capability
- Additional reference data provided (CVE, Bugtraq, etc.)
- Incident annotation/auditing
- Centralized management console

HIGH AVAILABILITY

- Automatic failover and failback
- High-speed failover
- "Five nines" (99.999%) reliability
- Cost-effective high-availability deployment configurations

DEPLOYMENT

- Multiple interface support (Gigabit and Fast Ethernet)
- Easy to deploy and install
- Non-intrusive deployment (non-inline)
- VLAN-aware detection
- Minimal training requirements

REPORTING

- Integrated deep drill-down console reporting
- Web-based reporting
- SQL export
- Automate reporting
- Customized reporting

HARDWARE REQUIREMENTS

- Multiple sensors per unit
- Multi-processor scalable

*Evaluation Test Template created by Brian Hernacki, Architect, Symantec Corporation

> **About the Author**

Linda McCarthy is the Executive Security Officer, Office of the CTO. She was previously the VP of Systems Engineering for Recourse Technologies. She also served as the Senior VP for NETSEC and was the founder of Network Defense and Manager for Security R&D at Sun Microsystems.

SYMANTEC, THE WORLD LEADER IN INTERNET SECURITY TECHNOLOGY, PROVIDES A BROAD RANGE OF CONTENT AND NETWORK SECURITY SOFTWARE AND APPLIANCE SOLUTIONS TO INDIVIDUALS, ENTERPRISES AND SERVICE PROVIDERS. THE COMPANY IS A LEADING PROVIDER OF VIRUS PROTECTION, FIREWALL AND VIRTUAL PRIVATE NETWORK, VULNERABILITY ASSESSMENT, INTRUSION PREVENTION, INTERNET CONTENT AND EMAIL FILTERING, AND REMOTE MANAGEMENT TECHNOLOGIES AND SECURITY SERVICES TO ENTERPRISES AND SERVICE PROVIDERS AROUND THE WORLD. SYMANTEC'S NORTON BRAND OF CONSUMER SECURITY PRODUCTS IS A LEADER IN WORLDWIDE RETAIL SALES AND INDUSTRY AWARDS. HEADQUARTERED IN CUPERTINO, CALIF., SYMANTEC HAS WORLDWIDE OPERATIONS IN 38 COUNTRIES.

FOR MORE INFORMATION, PLEASE VISIT WWW.SYMANTEC.COM

WORLD HEADQUARTERS

20330 Stevens Creek Blvd.
Cupertino, CA 95014 U.S.A.
408.517.8000
800.721.3934

www.symantec.com

**For Product information
In the U.S. call toll-free
800.745.6054**

**Symantec has worldwide
operations in 38 countries.
For specific country
offices and contact numbers
please visit our Web site.**