MP 00B0000046

MITRE PAPER

Intrusion Detection System Requirements

A Capabilities Description in Terms of the Network Monitoring and Assessment Module of CSAP21

September 2000

Therese R. Metcalf
Leonard J. LaPadula

Sponsor: Air Force Electronic Systems Center
Department: G037, G021
Contract: F19628-C-99-0001
Project: 03007499-00

MITRE
Center for Integrated Intelligence Systems
Bedford, Massachusetts

Abstract

This paper presents the intrusion detection and vulnerability scanning capabilities that the authors consider necessary for the U.S. Air Force network. These capabilities are described as requirements for the Network Monitoring and Assessment (NMA) module of the Computer Security Assistance Program for the Twenty-First Century (CSAP21) architecture. The advantage of this approach is that it provides a global and comprehensive context in which to describe intrusion detection system (IDS) requirements. We have adapted and organized requirements derived from a number of sources, including intrusion monitoring practitioners.

KEYWORDS: intrusion detection, vulnerability scanning, requirements, architecture, IDS, intrusion detection system, network monitoring and assessment, NMA, CSAP21

Acknowledgments

We thank Lori Gill, Office Coordinator in G021, for her thorough copy editing of our final draft.

Table of Contents

Section 1

Introduction

This paper identifies high-level system requirements for Air Force intrusion detection systems.

Background

These requirements are presented as Network Monitoring and Assessment (NMA) module high-level system requirements. The NMA is a major component of the Computer Security Assistance Program for the 21st Century (CSAP21) system of systems structure[1]. The NMA module's purpose is to collect and analyze cybersecurity monitoring (CSMn) data, providing centralized management and correlation of Air Force monitoring data, thus supporting comprehensive protection across all access paths of the Air Force network.

In CSAP21, requirements are developed within a framework of modules. A module is a grouping of functionality and capabilities into a logical processing unit. Modules are grouped into three functional areas:

- Data Gathering
  - Intelligence and Threat Correlation (ITC) Module—Deals with intelligence information relating to cyberthreats to the Air Force network; in this context, intelligence information consists of threat, vulnerability, and countermeasure data
  - Network Monitoring and Assessment (NMA) Module—Collects and analyzes Intrusion Detection and Reaction (IDR) data
  - CSAP21 Network Mapping (CNM) Module—Supports network management through application of mapping capabilities—gathering and displaying identification and status information about Air Force-wide information technology assets
- Decision Support
  - Situation Assessment (SA) Module—Assesses the state of a given system and develops information protection status and ongoing situational awareness
  - Risk Analysis (RA) Module—Analyzes risk associated with suspicious activity or system status and provides recommended courses of action
  - Modeling and Simulation (M&S) Module—Supports the SA and RA modules, providing "what if" scenario functionality

[1] The NMA and other modules are described in *CSAP21 Functional Requirements*, Therese Metcalf, The MITRE Corporation, September 1999. The referenced document is an internal Working Note, not available to the public. However, the reader does not need it for understanding the requirements delineated in this paper.

- Data Storage
  - CSAP21 Database System (CDS)—This data repository module provides the logical data store for all other modules

The original compilation[2] of NMA requirements had the purpose of guiding development. The current paper has the same general goal, expanded to include research, design, and implementation by vendors of commercial products, contractors developing capabilities for the Department of Defense (DOD), and government efforts producing prototypes, proofs-of-concept, or government off-the-shelf capabilities.

Disclaimer

The United States Air Force makes no claim that the requirements in this paper represent official requirements of the United States Air Force. They are rather the product of the best professional judgement of the authors of this paper, based on their understanding of Air Force needs.

Scope

This paper is a statement of needs, focusing on intrusion detection system (IDS) functional and performance requirements. These requirements are grouped into five categories

- Processing requirements
- Functional requirements
- Output requirements
- Technical requirements
- Miscellaneous requirements

Performance requirements are included throughout these categories but are limited in definition since the best of available technology is the capability sought.

[2] A list of documents used in the original compilation is included in the Bibliography of this paper. Most of them are not in the public domain. Again, these documents are not needed to understand or use the content of this paper; the references to them are included to foster confidence that the current requirements have a sound basis.

Section 2

Processing Requirements

The NMA module has three high-level processing activities: monitoring, an activity of the sensors; assessing, an activity of the analyzers; and managing, an activity of the directors. These processing activities are described here from a relatively high-level point of view. The same capabilities are discussed in greater detail under Functional Requirements.

Monitoring

The NMA module provides comprehensive monitoring for intrusion and vulnerability detection. The NMA must monitor all traffic and must scan all hosts across Air Force networks. To provide the needed functionality, the NMA module accepts data from many intrusion detection sensors and vulnerability scanners. In this context, sensors and scanners may be complete intrusion detection and monitoring systems since the NMA is a hierarchically composed system of systems. The intrusion detection and vulnerability scanning systems monitor and collect data at different levels

- At the site level
  - One or more IDSs can monitor network traffic from several locations within the site network and collect intrusion detection and vulnerability data at several locations within the site network
  - An IDS can collect intrusion detection and vulnerability data at a centralized place from all other site intrusion detectors
- At the federated level, one or more IDSs can collect intrusion detection and vulnerability data from the sites—at the intermediate level, an IDS can collect data from sites that are logically organized into regions, at the global level, an IDS can collect data from all regional collectors and all sites not covered by regional collectors

The NMA in aggregate provides intrusion and vulnerability detection and characterization. It uses both the misuse and anomaly detection models on computers and networks. Its sensors continuously collect network- and host-based data without direct control of a manager. They monitor the information flows across commands' perimeters and within commands' intranets, selectively capturing and recording traffic for analysis and archive. They collect data from hosts' operating system logs, audit trails, network interface cards, and so forth. This includes firewalls, routers, and such as sources of intrusion and vulnerability data.

Intrusion detection sensors should meet the data collection requirements without dropping network packets—that is, they should have adequate performance to keep up with whatever networks or hosts they are monitoring. In addition, they should not be detectable by an attacker.

Assessing

The NMA module provides comprehensive analysis of intrusion and vulnerability data. Assessment components may be co-located with or integrated into either the sensors or directors of the NMA module. These components will translate, analyze, and correlate data for operational support and for interaction with the other CSAP21 modules, including countermeasure assessment, trace-back, auto-response, or course of action development.

The NMA module will correlate data from multiple sources to identify suspicious activity and patterns of vulnerability and exploitation. Analysis capability should be able to operate on historical data and should also be able to operate in real or near-real time to assess the current state of the network. This ability should be available at both the site and federated levels.

The NMA module must perform damage assessment, including making estimates of extent of damage to information assets, time to recovery, actual and potential impact on the network. The NMA module may use forensic analysis tools in doing the damage assessment to ensure that needed data is available in a usable form for subsequent investigation or prosecution.

Managing

The directors/managers of the NMA module need to provide performance management, fault management, and security management of the IDS resources under their control. They must monitor and report the state of health of their sensors—this ideally will be achieved through some standard health-status reporting protocol between the sensors and their directors/managers. The directors/managers must maintain configuration information about their sensors and about inferior directors/managers that report to them. They must also be able remotely to control and update their sensors.

Section 3

Functional Requirements

The NMA module needs to perform a variety of functions. We have grouped these functions into several categories covering collecting, processing, analyzing, reporting, and storing intrusion and vulnerability data, providing alerts, displaying information, controlling IDS resources, reacting to intrusions and vulnerabilities, and interacting with other CSAP21 modules. These functions provide lower level requirements than the processing requirements of the previous section.

Collecting

The NMA module collects intrusion detection and vulnerability data. For intrusion detection in both real time and non-real time, the NMA module needs to

- Collect suspicious traffic and ancillary information that describes or characterizes the traffic, identifying distinct network connections or associations (connectionless traffic) and including enough detail to assist criminal investigations and prosecutions
- Detect intrusions specific to a designated area of protection
- Detect denial of service attacks to include service overloads, broadcast storms, and message flooding
- Automatically record events and incidents
- Monitor and scan networks
- Monitor and scan hosts
- Detect based on content; for example, a packet body
- Detect based on context; for example, a packet header
- Detect intrusions for multiple operating systems
- Detect intrusions for multiple platforms (hosts, switches, routers, etc.)

For vulnerability detection, the NMA module needs to

- Scan networks
- Scan hosts
- Detect vulnerabilities for multiple operating systems
- Detect vulnerabilities for multiple platforms (i.e., hosts, switches, routers, etc.)

Processing

The NMA module processes intrusion detection and vulnerability data. At sensors and/or directors/managers, it needs to

- Perform data reduction, preferably at the source, to lessen data load
- Refine raw data to eliminate redundancy and false alarms

These capabilities are intended to mitigate operator and system overloading.

The NMA module provides a general capability for operators to manage the intrusion detection and vulnerability data, including

- Capability to create reports for following up on and taking corrective action on suspicious events or discovered vulnerabilities not getting immediate attention
- Capability to open, track, and document resolution of an intrusion incident or discovered vulnerability
- A site profile database, to be used by an operator to maintain a record of site-specific activity

Ideally, the NMA at every level of the enterprise will employ a single standardized interface to operators.

Analyzing

The NMA module analyzes intrusion detection and vulnerability data. At sensors and/or directors/managers, it needs to

- Identify the vulnerability exploitation type of a discovered vulnerability (for example, component, protocol, application, and configuration) and provide information relevant to remedying the vulnerability—whether a remedy is available, what it is, how to apply it, and so forth
- Correlate raw or refined data, such as associating multiple attacks occurring at different targets with the same source and associate system vulnerabilities with attacks
- Aggregate inputs from several sources of the same type into a single incident report and fuse inputs from several sources of disparate types and possibly differing security levels into a single situation report
- Aggregate threat, vulnerability, and countermeasure data to support other functions, such as trend analysis and next-target prediction
- Analyze/decode events on some protocols or services that are normally not readable by a human (for example, NetBios [ports 137, 138, and 139], Network File System (NFS), and rpcinfo calls) and put them into human-readable form
- Provide both local and remote data analysis tools

Ideally, the NMA at every level of the enterprise will employ a single standardized interface to analysts.

Reporting

The NMA module reports intrusion and vulnerability data. Suspicious event reports should automatically be logged in a data store. The NMA should have the capability to send reports to designated recipients.

Reports should provide the following kinds of information for intrusion incidents:

- Description of the suspicious event identified
- Keystroke data from the initiating host, and the keystroke data from the receiving host (i.e., provide sufficient supporting data to allow an operator to understand the context of the suspicious event being reported); this transcript can be generated at the time of the incident or can be generated from captured data at a later time
- Connections logs for all ports and services for all the network data collected; the connections log must identify as a minimum the following for each network connection recorded:
  - Unique identifier of the connection
  - Protocol or service
  - Port used by the initiating host
  - Port used by the receiving host
  - Start time of the connection
  - Duration of the connection
  - Number of packets the initiator sent
  - Number of packets the receiver sent
  - Number of bytes the initiator sent
  - Number of bytes the receiver sent
- Operational reports detailing the status of ongoing cybersecurity operations, results of previous operations, and plans for future operations

The system must be capable of operating in an hierarchical reporting structure

- A sensor must be capable of reporting to a manager
- A manager must be capable of reporting to other managers
- Multiple sensors must be capable of reporting to the same manager and multiple managers must be capable of reporting to a top-level enterprise manager

Warning

- The NMA should provide real-time alerts for suspected intrusions, displayed to a user console[3]; these should be configurable as visual, aural, or both. Alerts provided by the NMA should be easy to understand and should be implemented in such a manner as to avoid operator and system overloading. Alerts should be graded; for example, as “cautions”, “warnings”, and “alarms”. Operators should have the ability to select alerts based on their grading. In addition, the NMA should have the capability to simultaneously activate multiple notification components (for example, e-mail, log, display, pager, or aural indicator).
- Similarly, the NMA should provide alerts to the operators for suspicious events identified by the analyzer components of the NMA

[3] The user console can and normally should be implemented in software.

- Alerts, whether generated in real time or as a result of analysis, should include, as a minimum, the following information
  - Source IP address
  - Destination IP address
  - Source port and service
  - Destination port and service
  - Actual or estimated start and end times of event
  - Description of suspicious event; this description should include a unique identifier by which the suspected intrusion can be referred too unambiguously
- The NMA should have the capability to send warnings to appropriate organizations; for example, send, through cyberspace, a warning characterizing an attack to defined recipients (for example, Air Force Computer Emergency Response Team (AFCERT) and the system owner that is at risk)

Displaying

The NMA needs capabilities to display both real-time and processed intrusion and vulnerability data. The NMA should provide

- Capabilities to
  - View the data stream in real time (for example, observing or "tailing" network session activity in real time)
  - View alerts in real time
  - Play back a saved Transport Control Protocol (TCP) or other session
  - Display the results of analysis of intrusion and vulnerability data
- A local level console where local data and reports can be accessed and reviewed; this can be at the sensor console or by secure remote access to the sensor
- An enterprise level console where all capabilities can be accessed and controlled
- The ability to view information in graphical form, such as network layouts, network components, inter-network connections, various statistical data from reports, and so forth
- Both
  - A desktop display that visualizes detailed information for an area of responsibility such as a base, theater, or region
  - A global display that visualizes the global Air Force information protection situation

Controlling

The NMA module controls the intrusion and vulnerability detection and scanning resources. The directors/managers of the NMA module provide performance, fault, and security management of the IDS resources under their control. They must

- Monitor the state of health of the sensors under their control; when a director/manager detects a failed sensor, it must alarm the operator
- Report the state of health of their sensors to predetermined authorities
- Control their sensors by directing their behavior in accord with changing situations; this requires that sensors be built with a set of commands that they know how to carry out
- Update their sensors, with new signatures for example, when the sensors are unable to receive automatic updates
- Maintain configuration information about their sensors and about inferior directors/managers that report to them; this configuration information should reflect the state of a sensor that has carried out a command of its director/manager

The communication among sensors and directors/managers ideally will be achieved through some standard health-status reporting and command protocol. Ideally, the NMA at every level of the enterprise will employ a single standardized interface to managers of the NMA resources.

Reacting

The NMA module needs capabilities to respond to attacks and discovered vulnerabilities by either carrying out recovery, restoration, and reconstitution activities or providing information in support of such activities. These capabilities are for recovering from attacks, reconstituting resources to ward off attack or ameliorate vulnerabilities, and restoring disabled capabilities. In general, these capabilities allow the NMA module to participate in enforcing a network security policy. These capabilities can be met by sensors, directors/managers, or both.

- Responses to events should include the ability to deny, degrade, disrupt, and deceive the attacker; to reconfigure systems and information functions, and to counterattack. For example, the NMA should be able to take control of a connection or association (for example, connectionless traffic between two systems using the user datagram protocol [UDP]); it must be able to terminate connections, effectively denying access to a network or host; it must be able to redirect a connection to a decoy, denying access to a network or host but allowing the connection to remain under observation. It must be able to react to an apparent denial of service attack, such as service overloading, broadcast storming, or message flooding, to limit its effectiveness.
- The NMA module should be capable of initiating appropriate automated responses to an event, alert, or incident; such as recording, reporting, closure of session,

shunning[4], and filter updates; the ability to react to suspected intrusions should include capability to take a predetermined action and to present an administrator with a list of candidate responses

- NMA sensors should be capable of turning themselves off and being turned off in response to predefined conditions
- For responding to suspicious events,[5] the NMA should have configurable capabilities or features
  - To track and log activity across all ports and services of an internet protocol (IP) address identified as associated with the suspicious activity
  - To automatically react with predefined defensive techniques and procedures for recovery and reconstitution
  - To block for a configurable period of time any port or service associated with an identified suspicious activity
  - To shun an IP address with respect to continued activity once the IP address is identified as being associated with suspicious activity
- The NMA should have a capability for logging the response taken for each real-time alert

Storing

- The NMA should have the ability
  - To feed information about verified intrusions and vulnerabilities to a central (single logical) database for analysis and long-term storage
  - To use distributed database capability with the attendant ability to feed data from one to another
  - To feed "up" to the centralized database from distributed databases
  - To feed "down" from archival storage at the centralized database to enable certain kinds of analysis (for example, to discover whether a particular attack that is being investigated at an air base has been seen in the past six months at any of the fixed air bases in Europe, to review a sequence of networking events involved in an attack, or to test new detection criteria against a sequence of events)
- The central database capability should
  - Provide data sorts and queries and should have backup capability
  - Store data for up to three years
  - Store processed data in a format usable by the other CSAP21 modules
- Sensors should have the capacity to store seven days of raw network traffic locally and to automatically back up traffic as needed

---

[4] To shun an IP address requires that any current activity associated with that IP address be stopped and future activity with that IP address as a source be denied.

[5] Including non-intrusive reconnaissance events

- Centralized management components of the NMA should have
  - Capacity to store 90 days of collected enterprise data[6] for immediate access and analysis in the manager
  - Capability automatically to back up 365 days of collected enterprise data in the manager, with capability for an operator to retrieve and review this historical data

Interacting

The NMA module interacts with other CSAP21 modules.

The NMA module gets support from the ITC module for analysis of detected anomalies on the basis of both network-derived and traditional intelligence. This kind of analysis helps to assess the nature and magnitude of specific attacks. Network-derived intelligence is associated with context monitoring, which creates a collection of information publicly available to legitimate users. It is used to infer user activity without the need to collect and record actual keystrokes. In comparison, traditional intelligence is associated with content monitoring, collecting every keystroke entered by a user.

The NMA module generally supports the Decision Support modules in overall information protection operations The NMA module will directly support the RA and SA modules through vulnerability and incident data stored in the CDS. Network-derived intrusion data is exchanged with the RA module, through the logical data store, for timely analysis. This data is also shared with the SA module for correlation with other intelligence data.

The NMA module uses information generated by the CNM to determine critical nodes—those that are critical to maintaining operational status and should, therefore, be given highest priority for protection, recovery, reconstitution, and so forth.

[6] This is data reported to the manager from child managers, network sensors, and host sensors.

Section 4

Output Requirements

In providing the needed functionality and processing in the CSAP21 context, the NMA must generate several outputs. The outputs identified here are very general in nature—they must be further delineated for specific requirement specification and design. They will contain information from the requirements already defined. The outputs are organized into Attacker Profile, Security Profile, and System Profile.

Attacker Profile

The Attacker Profile output provides available data about an attacker—intruder or prober, whether an outsider or insider. This output contains the following information:

- Trace results: report of track/track-back results
- Cyber point of origin: identification of the origin of the attack in cyberspace
- Event tracking: script of activities the intruder engaged in and at what locations
- Service(s) used: the method of exploitation, such as component, protocol, application, or configuration vulnerability
- Attacker status: for example, uncontrolled, isolated, contained, and so forth

Security Profile

The Security Profile output provides detailed security information about a selected network domain.

System Profile

The System Profile provides information on what areas—address, components, and/or systems—are impacted. This output contains the following information:

- Address identifier: a cyberspace address, such as IP address
- Component(s): identification of hardware components that were compromised
- Software: description of the platform software—applications, system software, operating system

Section 5

Technical Requirements

The needs identified here are presented without consideration of implementation feasibility. They should be considered and provided where feasible.

General

- Implementation
  - Software-only implementation—systems implemented in software for various platforms are preferred over systems requiring vendor-specific hardware
  - Fault tolerant, in the sense that NMA capabilities must survive a system crash and not require their knowledge bases to be rebuilt at restart
  - Systems that can run under various operating systems (for example, Windows and UNIX) are preferred
  - Systems that are Defense Information Infrastructure Common Operating Environment (DII COE) compliant are preferred
  - Interfaces of the NMA to databases (for example, the CDS) must be open database connectivity (ODBC) compliant
- Performance
  - Monitoring and scanning systems should have no noticeable effect on normal network operations
  - Policy-enforcing systems should cause minimal degradation of normal network service
- Standards
  - Industry standards-based should be used; for example, systems should meet, or plan to meet, a standard interface for data interfacing and sharing, plan to meet standards set by the Internet Engineering Task Force (IETF), especially for inter-module data communications
  - A common mechanism and format is desirable for reporting up and down the enterprise-wide intrusion detection hierarchy
  - Systems should provide industry-standard graphical user interfaces(GUIs)

Network

- Systems should impose no significant load on local area network (LAN) or wide area network (WAN) bandwidth
- Products should be highly scalable to large networks across a large enterprise; the NMA in aggregate must be capable of receiving, handling, and storing data from an Air Force enterprise of 200 class B networks located around the world

- The NMA components must operate in the context of high-speed networks with high data volumes in multiple media; for example, Ethernet and Fiber Distributed Data Interface (FDDI) are widely used
- Systems should have the capability to establish alternate communications among components; for example, if normal network connectivity is lost, a manager might access a sensor via a modem
- Products should have minimal impact on local addressing schema

Security

- Systems should be secure against unauthorized access to any of their data, unauthorized use of them or any of their components, unauthorized distribution of any of their parts, and cyber attacks aimed at them
- Components of the NMA should ensure trusted relationships among themselves; for example, a sensor might authenticate itself to a manager and vice versa
- Products should use secure and reliable two-way data communications among components of the NMA; the system should use encryption and digital signatures when reporting

Section 6

Miscellaneous Requirements

An assortment of requirements addressing areas such as architectural and general performance characteristics, configuration capabilities, evolution considerations, and so forth are listed in this section.

Architecture

- NMA components should be adaptable to either centrally controlled operation or autonomous operation; moreover, this adaptability should extend from the lowest to the highest organizational levels; for example, many of the capabilities of the NMA will be centrally operated, controlled, and managed, but the NMA must also be capable of centralized operation from an alternate deployed operations center; at the same time, instances of these same capabilities must be capable of operating as an autonomous system, with its own central control, at the site or even lower level
- Redundancy of critical resources composing the NMA capabilities should be possible
- NMA components should be configurable from more than one control location
- Both networked and dial-in access to the control systems should be provided
- Control unit(s) should be capable of operating independently of other control units, even if connection to a central server, if any, is lost
- Overall, the NMA will ideally be capable of both hierarchical and distributed operation

Configuration

- Overall the NMA module must be configurable to perform intrusion detection based on the misuse detection model or based on the anomaly intrusion detection model; for the misuse detection model, this includes the requirement to perform both network content and network context analysis
- Systems should be configurable for detection and reaction, as feasible for alerts, filter updates, protocol and port coverage, and detection-threshold levels
- Systems should be configurable treat identified IP or other network addresses exceptionally; for example, configurable to never block or shun network activity from one or more IP addresses

Evolution

- Products suitable for inclusion in the NMA module should be engineered to allow easy integration of new functionality and capability as threats, technologies, and techniques evolve

Interfaces

- The NMA should be capable of accepting, assimilating, storing, and analyzing data from other managers, and from host-based and network-based intrusion detection and vulnerability scanning products

Duty Cycle And Robustness

- The NMA must support 24-hours-a-day, 7-days-a-week operations
- The NMA must have sufficient reliability to ensure continuous monitoring
- The NMA should have capability for both manual and automatic recovery after failure

System Updates

- Capabilities should be provided for adding, deleting, or modifying intrusion profiles in intrusion detectors; adding and deleting vulnerability descriptions in vulnerability scanners; automatic upgrading to new releases of products
- These capabilities should be engineered in such a manner as to allow updates during operational use of the products without disruption

Ease Of Use

- Operator console should not require undue expertise to operate; experts may reside external to operator staff, experts may reside external to operator staff
- GUIs provided for operators should be as intuitive and as easy to use as possible
- The NMA should be easy to restart after failure

Section 7

Related and Future Functionality

The capabilities listed here are either closely associated with other CSAP21 modules or are potential future capabilities of the NMA module; they should be considered when attempting to meet NMA requirements. For those associated with other CSAP21 modules, the NMA module would provide a primitive real-time or near real-time version of the capability, with refinement provided later by another CSAP21 module.

Capabilities Associated with Other CSAP21 Modules

For the capabilities listed here, the NMA potentially could provide a first-cut estimate, report, assessment, and so forth, with full capability provided by other CSAP21 modules.

CNM-Related Capabilities

The NMA could have capabilities to perform the following functions:

- Network performance monitoring for both internal[7] and externally connected[8] network activity
- Monitoring of information functions, including monitoring deployed locations from the continental United States (CONUS)
- Automatic monitoring of communications and system equipment status, with recording and display of results

ITC-Related Capability

The NMA module could provide an estimate of an intruder's or attacker's potential capabilities, based on known methods and tools.

SA-Related Capability

The NMA module could have a capability to perform penetration testing and on-line surveys (OLSs) to identify systems, current performance, system configuration, and vulnerabilities

Future Capabilities

The following capabilities could eventually be included as part of the NMA module:

- Fraud detection
- Fault detection
- Crisis monitoring
- News story monitoring

---

[7] Internal activity is network traffic that originates and terminates within a site's network.

[8] Externally connected network activity is network traffic that either originates outside a site's network and terminates within the site's network or vice versa.

Bibliography

Activity Monitoring: Noticing Interesting Changes In Behavior, Tom Fawcett and Foster Provost, from: Proceedings of the fifth ACM SIGKDD international conference on Knowledge Discovery and Data Mining, San Diego, CA USA, 15 – 18 August 1999

Analysis Report on GOTS vs COTS, AFCA, 16 November 1998

Anomaly Detection and Reaction Capabilities for the Air Force Deployed Tactical Data Networking Infrastructures, MTR 99B0000037, L. J. LaPadula, The MITRE Corporation, Bedford, Massachusetts, August 1999

Applied Signal Technology (APSG) Solution Concept to CI MAP FY00 Needs, USAF ESC/IYW, January 1999

Characteristics of a Good Intrusion Detection System, COAST, June 1998

Compendium of Anomaly Detection and Reaction Tools and Projects, MP 99B0000018, L. J. LaPadula, The MITRE Corporation, Bedford, Massachusetts, March 1999

CSAP21 Functional Requirements, Therese Metcalf, The MITRE Corporation, September 1999

CyberStrike Roadmap— Part 1: Information Protect Framework for Intrusion Detection and Reaction, Deborah J. Bodeau, MITRE Technical Report, September 1998

CyberStrike Roadmap— Part 2: Intrusion Detection and Reaction Architecture and Capabilities, Leonard J. LaPadula, MITRE Technical Report, December 1998

Defensive Counter Information (DCI) Operational Requirements Document (ORD), Air Material Command (AMC), August 1998

Information Assurance (IA) Automated Intrusion Detection Environment (AIDE) Advanced Concept Technology Demonstration (ACTD), Notes from attending meetings

Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection, Ptacek/Newsham, January 1998

Intrusion Detection for Air Force Networks: Operational, Performance, and Implementation Goals, L. J. LaPadula, MITRE Technical Report, August 1997

Intrusion Detection Message Exchange Requirements, RFC IETF, draft September 1999

Intrusion Reaction: Recommendations for Obtaining Reaction Capabilities, MTR 98B0000066, L. J. LaPadula, The MITRE Corporation, Bedford, Massachusetts, September 1998

Requirements Document for an Automated Global Intrusion Detection System, AFIWC/EA,December 1996

State of the Art in Anomaly Detection and Reaction, MP 99B000020, L. J. LaPadula, TheMITRE Corporation, Bedford, Massachusetts, May 1999

Glossary

Acronyms

AFCERT	Air Force Computer Emergency Response Team
CDS	CSAP21 Database System
CNM	CSAP21 Network Mapping Module
CONUS	Continental United States
CSAP21	Computer Security Assistance Program for the 21st Century
CSMn	CyberSecurity Monitoring
DII COE	Defense Information Infrastructure Common Operating Environment
DOD	Department of Defense
DOS	Denial of Service
FDDI	Fiber Distributed Data Interface
GUI	Graphical User Interface
IDR	Intrusion Detection and Reaction
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IP	Internet Protocol
ITC	Intelligence and Threat Correlation Module
LAN	Local Area Network
M&S	Modeling and Simulation Module
NIC	Network Interface Card
NFS	Network File System
NMA	Network Monitoring and Assessment
ODBC	Open Database Connectivity
OLS	On-Line Survey
RA	Risk Analysis Module
SA	Situation Assessment Module
SNMP	Simple Network Management Protocol
TCP	Transport Control Protocol
UDP	User Datagram Protocol
WAN	Wide Area Network

Definitions

The following are definitions for needed IDS functionality as well as for terms used in this document.

Activity: Events occurring at a data source that are identified by a sensor or analyzer as potentially constituting authorized or otherwise anomalous behavior (for example, network sessions, user activity, and application events).

Administrator: The human with some responsibility for setting the security policy of the organization, and, thus, for decisions about deploying and configuring an IDS. This may or may not be the same person as the operator of the IDS. In some organizations, the administrator is associated with the network or system administration groups. In other organizations, it is an independent position.

Alert: A message from a detector, scanner, or analyzer to a director or manager or administrator or user that a suspicious event has been detected. An alert typically contains information about the activity involved, as well as specifics relating to the detected anomalies.

Analyzer: A component or process that analyzes data collected by sensors for signs of unauthorized or undesired activity or for events that might be of interest to the security administrator. An analyzer may receive inputs from a variety of sources (for example, intrusion detectors, vulnerability scanners, and so forth), possibly from widely disparate and distributed sources, and may analyze the aggregated data to discover one or more things such as widely distributed attacks, distributed but coordinated attacks, patterns of vulnerabilities, and so forth.

Anomaly Detection Model: The intrusion detection system detects intrusions by profiling normal host or network activity and subsequently looking for activity that is different than the user's or system's normal behavior.

Data Source: The raw information that an intrusion detection system uses to detect unauthorized or undesired activity. Common data sources include, but are not limited to, network packets, operating system logs, application logs, and system-generated checksum data.

Denial-of-Service (DOS) Attack: A DOS attack is an attack against a computer system that is intended to compromise its availability.

Evasion Attack: An evasion attack is an attempt to bypass an IDS monitoring a computer network by sending a network packet that the IDS will ignore but that will be accepted by the receiving system. The intended result is for the IDS not to see an attack on the receiving system.

Event: An occurrence or pattern in a data source that is recognized by a monitor/sensor as being suspicious and that may cause it to alarm; for example, three failed logon attempts in 10 seconds might indicate a brute-force logon attack.

False Negative Error: Failure of an intrusion detector to alarm on an activity that is unauthorized or threatening—that is, an activity that the detector is intended to identify as suspicious.

False Positive Error: An intrusion detector's alarming on an activity that proves to be authorized or non-threatening activity when validated.

Federated Level: The intermediate or global level.

Host-based: Audit data or network interface card (NIC) data from a single host is used to detect intrusions.

Intrude: Gain unauthorized access to a computer or network, cause an undesirable change in data in a computer or network, or render a computer or network or one of its services unusable.

Intrusion Detection System: An integrated collection of one or more of the following components: monitor/sensor, assessment/analyzer, and manager/director.

Intrusion Detection: The activity of detecting attempts to intrude into a computer or network by observation of actions, security logs, or audit data.

Intrusion Incident: A validated occurrence of unauthorized access to a computer or network system.

Manager: The cybersecurity monitoring component or process from which the operator manages the various components of the cybersecurity monitoring system. Management functions typically include, but are not limited to, sensor configuration, analyzer configuration, event notification management, data consolidation, and reporting.

Misuse Detection Model: The intrusion detection system detects intrusions by looking for activity that corresponds to or correlates with known intrusion techniques—signatures—or system vulnerabilities.

Near-real Time: An action is considered to occur in near-real time when there is no more than a short delay between the triggering event and the action. For automated systems in the context of intrusion detection, we consider a delay time of 1 to 5 minutes to be near-real time.

Network Content Analysis: The analysis of network traffic by looking at the packets of a network packet stream to identify suspicious activity—typical of “string-matching” intrusion detection techniques. Network content analysis is typically based on a known signature and falls under the misuse detection model.

Network Context Analysis: The analysis of network traffic by looking across network ports and services to identify suspicious activity—typical of techniques used to identify port scans and ping sweeps. Network context analysis typically is based on some known technique and falls under the anomaly detection model.

Network-based: Network traffic is used to detect intrusions.

Notification: The method by which an IDS makes an operator aware of an event occurrence. In many IDSs, this is done by displaying a colored icon on the IDS console, the transmission of an e-mail or pager message, or the transmission of a Simple Network Management Protocol (SNMP) trap, although other notification techniques are also used.

Operator: The person that is the primary user of an IDS manager. The operator often monitors the output of the IDS and initiates or recommends further action.

Real Time: An action is considered to occur in real time when there is no appreciable delay between the triggering event and the action. For automated systems in the context of intrusion detection, we consider a delay time of less than a minute to be real time.

Response: The actions taken in response to an event. Responses may be initiated automatically by some entity in the IDS architecture or may be initiated by a human. Providing a notification or alert to an operator is a very common response of an IDS. Other responses include, but are not limited to, logging activity, recording raw data from a data source that characterizes an event, terminating a network, user, or application session, and altering network or system access controls.

Security Policy: The predefined, formally documented statement that defines what network services are allowed across the monitored segment of the network to support the organization's requirements. This includes, but is not limited to, which hosts are to be denied external network access.

Sensor: The intrusion detection component that collects data from a data source.

Signature: A specific characteristic of a transmission, message, or network packet being received that an intrusion detector associates with suspicious activity. Signatures are normally stored as patterns of data; the IDS uses them in a pattern matching process.

Site Level: The local unit or site level.

Subversion Error: Subversion errors are more complex and tie in with false negative errors. An intruder could use knowledge about the internals of the intrusion detection system to subvert its capability to identify suspicious activity. One example of this is to conduct an attack "low and slow," wherein the intrusion detection system may see individual events that seem not to pose a threat, but taken in aggregate pose a threat to system integrity.

Transcript: A report that contains the keystroke capture data from both the initiating host and the receiving host involved in a suspicious network connection.