MTR 97B0000035

MITRE TECHNICAL REPORT

Intrusion Detection for Air Force Networks

Operational, Performance, and Implementation Goals

October 1997

Leonard J. LaPadula

Sponsor: Air Force
Dept. No.: G021
Contract No.: F19628-94-C-0001
Project No.: 03977452OB

MITRE
Center for Integrated Intelligence Systems
Bedford, Massachusetts

Abstract

Will developing intrusion detection capabilities meet the operational, performance, and implementation goals of the US Air Force? To help ensure that they will, the MITRE C2 Protect Mission-Oriented Investigation and Experimentation (MOIE) project is making Air Force goals for intrusion detection available to commercial interests that may develop capabilities.

This paper, a first cut at defining goals, capitalizes on customer and corporate experience with intrusion detection tools as well as knowledge of the problem domain. It creates an information base about intrusion detection, providing a framework for discussing, refining, and enhancing intrusion detection goals.

KEYWORDS: intrusion detection, operational goals, performance goals, implementation goals.

Table of Contents

List of Figures

List of Tables

Section 1

Introduction

The Command and Control (C2) Protect Mission-Oriented Investigation & Experimentation (MOIE) Project, sponsored by the Air Force, aims to develop and promulgate resources to counter information warfare (IW) threats to military C2 computer networks. One component of the threat dimension is exploitative intrusion activity. Even a cursory look at this area reveals that IW attacks are becoming easier to mount, assisted by easily available, user-friendly software and a growing community of hacker web sites and mailing lists.

Given the nature of the C2 mission, the rewards of a successful IW attack on our C2 systems invite the attempt at exploitation. At the same time, we estimate that the number of foreign countries with IW capabilities is increasing rapidly. Since military systems are typically connected to and dependent on public switched networks, they are accessible to an attacker's attempts at exploitation. Moreover, we know from actual investigations performed by AFIWC, ESC, DISA, FIWC, MITRE, and others that many of our C2 systems are vulnerable.

Purpose

One technological countermeasure is intrusion detection capability. Once detected, a variety of actions can be taken to thwart an attacker's intentions. In the recent past, intrusion detection capabilities have been developed by both governmental and commercial interests. These nascent capabilities, although a significant start, will surely grow and evolve rapidly over the next several years to become far more capable and easier to use than they are today. We can reasonably expect commercial interests to have a leading role in extending this technology. At the same time, it seems prudent to examine intrusion detection technology from the point of our military systems to ensure that the goals for those systems will be met and that the best capabilities will be available to meet the threats.

Will developing intrusion detection capabilities meet the operational, performance, and implementation goals of the US Air Force? To help ensure that they will, the MITRE C2 Protect Mission-Oriented Investigation and Experimentation (MOIE) project has been focusing on Air Force needs with a view to articulating them to commercial interests that may develop capabilities. This may help shape future funding decisions and may also provide a common framework for discussing issues.

This paper is based on combined customer and corporate experience with intrusion detection tools as well as knowledge of the problem domain. It provides a framework suitable for refining and enhancing intrusion detection goals as our collective understanding

of the problem and potential solutions improves. The time frame of the goals is limited to one to three years in recognition of the rapid evolution in both technology and the threat environment.

This first cut provides an information base about intrusion detection needs for military computer networks and desirable characteristics of the tools that will meet those needs. Besides providing guidelines for vendors, this information resource may assist the Air Force's participation in more global efforts such as development of the Automated Intrusion Detection Environment (AIDE) under the DoD Advanced Concept Technology Demonstration program. The information base may be useful to an Air Force mission area team[1] looking at intrusion detection needs. It should also assist planning for acquisition and funding and provide a common framework for addressing issues.

Protection Domain

An intrusion detection capability can be built to operate on and protect an individual host, workstation, router, gateway, or server. Such a capability would be limited in its scope of applicability to systems of the type for which it had been built. For some kinds of attacks, such a specialized capability might be the only feasible way to detect an attack. For convenience, we call this kind of capability a platform capability, where platform is understood to be a class defined by hardware and operating system types, such as PCs running Windows, workstations running UNIX, and so forth.

An intrusion detection capability can operate on a broader scale, protecting a defined set of resources that constitute a network. Although this might often be appropriately called an enterprise capability in the commercial world, we will call this a site capability to suggest the level of granularity we are talking about in the military setting. This should avoid confusing the scope with the entire Air Force network. A capability with this scope might or might not employ platform capabilities; if it does, it will naturally also perform an integrating function of some kind to create a more global picture of an attack than can be attained with individual platform capabilities.

An intrusion detection capability can operate on and protect an even larger network of some kind. We are, of course, interested in the global Air Force network. For convenience, we call this a federated capability, for the global Air Force network as well as networks of lesser scope whose distinct subnetworks coalesce functionally for intrusion detection. A capability with this scope will of necessity employ site capabilities as its agents, collecting and correlating their reports to detect and report federation-wide attacks.

---

[1] Mission area teams, part of the TPIPT (Technical Planning Integrated Product Team) process, identify deficiencies and investigate relevant technology. The TPIPT process marries deficiencies with recommended solution concepts, risk, and cost..

Envisioned intrusion detection operations cut across a wide range of systems employing numerous networking capabilities and computers, having different mission criticality, and processing various kinds of information ranging from unclassified to highly classified and from ordinary to highly consequential. These factors may impact performance requirements and influence implementation decisions for automated tools.

Scope

This paper addresses goals for site and federated capabilities. In practical terms, the desired capabilities need to work at both the global level and the level of Air bases and deployed forces. Although both of these ultimately depend on platform capabilities for detecting certain kinds of attacks and for detailed information about them, intrusion detection issues affecting military systems arise at the site (base/deployed force) and federated (global) levels of capability. At these levels, technical capabilities, policy, and administrative procedures will have to come together to produce an effective capability to thwart intrusive exploitative attacks. This paper does not examine specific methods for detecting intrusions, does not address preventive measures that might forestall intrusions, and, generally, does not attempt to put intrusion detection into a total security posture context. Delimiting the scope in this way focuses attention on global operations and the general performance and implementation characteristics of automated tools for intrusion detection.

Approach

We generally classify goals as operational, performance, or implementation goals. Operational goals describe the way the Air Force believes it will need to operate in dealing with intrusive exploitative attacks. Performance goals address what functions an intrusion detection capability should be able to perform and how it should go about doing those functions with respect to its network and its users. Implementation goals deal with the areas of maintenance, standards, security, and training. The next section provides an overview of expected Air Force intrusion detection operations; then this document lays out performance goals; the final section addresses implementation goals.

Section 2

Operational Goals

This section gives an overview of Air Force intrusion detection operations at the federated and site levels. Following the overview, several specific operational goals are described.

Overview

Air Force intrusion detection operations are two-tiered, in line with the natural hierarchy of military operations. Intrusion detection at the base and force level is essentially a real-time activity carried out in coordination with other security measures and execution of the mission. At the global level today an intrusion detection reporting and analysis system is in place and being enhanced. Over the next few years as more capable tools become available, global operations will include near real-time intrusion detection through correlation of multiple real-time inputs from lower echelons.

The Air Force Computer Emergency Response Team (AFCERT), established by the Air Force Information Warfare Center (AFIWC), Air Intelligence Agency, is the single point of contact in the Air Force for reporting and handling computer security incidents and vulnerabilities. In this role, AFCERT must coordinate the technical resources of AFIWC to assess, analyze, and provide countermeasures for computer security incidents and vulnerabilities that are reported by Air Force computer users, security managers, and system managers. Reliable, up-to-date information about incidents, vulnerabilities, and the resources affected by them is key to successful execution of this mission. Electronic Systems Center (ESC)/ICW plays an important role in assessing vulnerabilities of weapon systems. Its Vulnerability Assessment/Risk Management (VA/RM) program adds to the information about vulnerabilities and threats that is available to AFCERT and gives program managers guidance for mitigating the risks, for example by building-in security protection in new or upgraded systems.

The AFIWC monitors operations, providing a global view of the Air Force network's security posture and recommending actions to base and regional commanders based on this global view. It provides operational decision support to other Air Force, DoD, and national level information warfare decision makers. The AFIWC's AFCERT provides the overall Air

Force intrusion detection and incident response center for information protection (IP) operations[2].

An important part of the overall IP operations concept will be intrusion detection capability for the 107 Air Force bases as well as for deployed networks in various theatres of operation. An Air Force Network Control Center (AFNCC) is located at each base and provides the focal point for management and protection of computer networks.

The intrusion detection operational concept, then, is for AFNCCs and Information Warfare Squadrons (IWS) to do intrusion detection in real time to protect bases and deployed forces as well as provide alarms and reports to the AFCERT. The AFCERT will use its extensive information collection, including mission, criticality, and sensitivity information (AFIWC 96), to manage alarms and reports. By independently analyzing collected data to detect exploitative activity on a global scale, the AFCERT operation will give deployed forces a potentially decisive information warfare advantage.

Detection

The operational goal is to recognize and report all activities that may be exploitative. Exploitative activity includes

Adversely affecting operations, including compromise of Air Force intentions and capabilities

Denying or degrading service to authorized users

Modifying information to adversely influence operations

Reducing the confidence of the US public or leadership in the capability of the Air Force to carry out its mission

Analysis

The operational goal for analysis is for each AFCERT analyst to spend no more than 30 minutes per day per AFNCC to analyze the reported data for the past twenty four hours. Current tools can require up to three hours per day per AFNCC.

Balancing False Negatives and False Positives

The ideal operational goal is to have no false negatives or false positives. With current and foreseeable technology, however, this is an unachievable goal. Moreover, an emphasis on reducing false positives runs the risk of increasing false negatives, and vice versa. For

---

[2] Information protection operations are proactive security functions established to assist Air Force organizations to deter, detect, isolate, contain, and recover from information systems and network intrusions.

example, Sandia National Labs (Sandia 1996) claims that for programs that detect anomalous behavior “False positives can be reduced, but only at the expense of increased false-negatives.” Since the ideal is not practically achievable, some reasonable balance should be struck. However, what may be reasonable at one time may not be appropriate at another time since the current mission and situation can drastically change priorities. The practical operational goal is to reduce false indications adequately for the intrusion detection capability to be useful, to provide a metric to the analyst indicating the probable current ratio of false negatives to false positives, and, very importantly, to allow an operator or administrator to adjust detection parameters to adapt the ratio to a changed situation.

Correlating Data Over Time

The AFNCCs should be able to correlate intrusion attempts from collected data retained on-site over a period of at least 96 hours back from current date. The AFCERT should be able to correlate activities from collected data at the AFCERT site over periods of up to three years back from current date. The AFCERT should be able to correlate specific activity recorded at an AFNCC to other activities recorded at the AFCERT over periods of up to three years back from current date. The latter capability should also be available to AFNCC operators on request, by sending, for example, an automated correlation request to AFCERT.

Access to Centralized Database

The AFNCCs should be able to get on-line access to the centralized archival data collection maintained at the AFCERT. This access is needed to allow data analysis by an off-line correlation process. “This process will correlate suspicious activity and incident data derived from intrusion detection with data from other sources over a period of at least three years.” (AFIWC 96)

Point of Origin Analysis

The operational goal is to identify the source of suspicious activities and incidents and to make the identification available to interested agencies (e.g., AFCERT, AFNCCs) as selected by system administrators within five minutes of identification. It is desirable for the identification process to be able to use one of three progressively more intrusive, and more powerful, methods, selectable by an operator. In each case the ideal is to do identify a source without letting the intruder know the source has been discovered.

Method 1: Identify the apparent source of activity using information available directly from captured network packets, without using intrusive methods. The operational concept is for this process to be done automatically, with results supplied with an initial suspicious activity report.

Method 2: Identify sources prior to the apparent source using nonintrusive tools and techniques. The operational concept is for this process to be configurable by a system

administrator or operator to be done either automatically or on specific approval of the operator. When configured to operate only on approval, the system should automatically generate a request to use the tools or techniques.

Method 3: Identify the source of activity using intrusive tools and techniques. The operational concept is for this process to be configurable by a system administrator or operator to be done either automatically or on specific approval of the operator. When configured to operate only on approval, the system should automatically generate a request to use the tools or techniques. In addition, the concept is for this process to be configurable to limit the types of services or systems that can trigger an automated response.

Section 3

Performance Goals

From discussions with users and builders of intrusion detection capabilities and from the nature of the problem domain itself, we see three classes of performance goals:

Functional: functional goals describe what an intrusion detection capability should do

Architectural: architectural goals indicate how a capability should fit itself to the network it will protect

Human Interface: human interface goals identify use characteristics of a tool

To ascertain goals in these three classes, one can

Identify types of exploitative activities for which intrusion detection is relevant and identify trends in these activities

Characterize the computer networks (technology, topology, connectivity) that will need protection from intrusive exploitative activity

Characterize the responsibilities and work environments of the administrators who will have to use intrusion detection tools

Corporate and sponsor experiences enable us to develop a preliminary version of the goals. We have used objectives identified by AFIWC (AFIWC-96), requirements developed by the AF 609 Information Warfare Squadron (McBrien 96), and goals implicit in the mission of the AF Computer Emergency Response Team (AFCERT 92). These organizations, especially the 609, have used tools in operational environments. We can extrapolate function, since we have studied the tools and technology of intrusion detection. We can interpret human interface needs, since we have a good understanding of our sponsors' responsibilities and work environments. We can use our knowledge of shortfalls in existing tools across all classes of goals, since we have evaluated tools. As time goes by, we expect to refine the goals as we gain experience with exploitative activities, computer networking, and sponsors' missions and operational objectives.

The idealized architecture shown in the appendix to this paper provides a backdrop for viewing these goals. We have stated goals whenever possible as goals to be met by "the system", by which we mean the components of the intrusion detection capability, taken collectively, at the level for which a goal is given.

Functional

The premier source of objectives for information warfare in the Air Force are the CINCs and the Chiefs of Staff. The Air Force Information Warfare Center (AFIWC) serves as a

clearing house for all Air Force experiences in the information warfare arena. One of its recent efforts has been to reflect those experiences in a draft objectives document for a global intrusion detection capability (AFIWC 96). Besides addressing high-level operational goals, this document identifies some functional goals for the federated level.

For functional goals relating to real-time operations at the force (site) level, we have used the intrusion detection needs specified by the Air Force 609 Information Warfare Squadron (IWS) (McBrien 9/96). The 609 needs a network monitoring system to conduct information defense operations for Ninth Air Force bases. The mission requires network monitoring of traffic through several base network gateways, on both classified and unclassified networks. Monitoring should detect exploitative activity at a detailed enough level to allow real-time response to the threat. Audit information gathered by the intrusion detection capability will be centrally collected at Shaw AFB for further analysis and stored for use in criminal or other proceedings and as an ID&D resource during wartime.

A similar situation pertains at numerous bases throughout the military. A typical military base has one or more local area networks (LANs) gatewayed to the MILNET or NIPRNET[3], sometimes also gatewayed to the Internet. In many cases both classified and unclassified LANs are in operation.

The goals and needs identified for today's missions and activities fit into the following categories of functional goals:

Monitor: to watch activity or conditions that are indicators of intrusive behavior

Detect: to identify activity or conditions that indicate an intrusion attempt

Capture: to record activity or conditions that indicate an intrusion attempt

Control: to actively determine the behavior of a network connection (e.g., connection hijack or terminate)

Collect: to gather records from several sources and organize them into a data store

Analyze: to examine captured information to decide a question such as "Was there an intrusion attempt?", "Where did the attack originate?", "What systems were affected by the attack?", and so forth

React: to take action in response to a perceived attack to achieve some goal

Notify: to present an alarm indication to one or more receivers

Report: to present a human-understandable description of a perceived attack

Store: to put information regarding intrusion attempts and attacks into long-term storage

[3] Military bases are gradually changing from using the older Military Network (MILNET) to the new, IP router-based, SBU segment of the Defense Information Systems Network (DISN) (NIPRNET).

Playback: to get information about an attempt/attack from long-term storage and report it

Table 1 presents near-term functional goals.

Table 1. Functional Goals

Category	Goal
Monitor	Able to monitor both internal and externally-connected network activity. Internal activity is network traffic that originates and terminates within the site's network. Externally-connected network activity is network traffic that either originates outside the site's network and terminates within the site's network or vice versa.
Detect	Able to perform both misuse detection and anomaly detection.
Capture	Able to make a copy of suspicious traffic and to record ancillary information that describes or characterizes the traffic. The capture should be able to identify distinct network connections or associations (connectionless traffic) and to include enough detail to assist criminal investigations and prosecutions.
Control	Able to take control of a connection or association (e.g., connectionless traffic between two systems using UDP). Control should allow the tool to terminate the connection, effectively denying access to the network, or to redirect the connection to a "spoofer" or similar system, again denying access to the network but allowing the connection to remain under observation. To be effective, control should be exercised in real time[4].

[4] 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*.

Category	Goal
Collect	At the site level: Able to collect intrusion detection information from all site intrusion detectors. At the federated level: Able to collect intrusion detection information from all sites.
Analyze	Able to analyze collected intrusion detection information. Analysis should be oriented toward identifying anomalies and misuse that have not been detected at the sources of the information (that is, at the places where network traffic was being monitored and captured). For example, an attack involving simultaneous probing of multiple hosts on a network might be detected by this kind of analysis. The analysis capability should be able to operate on historical data and should also be able to operate in real or near-real time[5] to assess the current state of the network. This ability should be available at both the site and federated levels.
React	Able to react to suspected intrusions by Taking predetermined action for the detected misuse or anomaly Presenting an administrator with a list of candidate responses
Notify	Able to report a suspected intrusion by activating one or more real-time alarms. Real-time alarms should be visual and aural. They should correspond to several levels of concern such as *cautions, warnings*, and *alerts*. Also able to activate a paging system and to simultaneously activate multiple notification components (e.g., email, log, display, pager, or aural indicator). The alarm indication, in whatever form, should include an identifier by which the suspected intrusion can be referred to unambiguously.
Report	Able to present a human-understandable description of a perceived attack, based on a suspected-intrusion identifier provided to the system. The description should include temporal and spatial information for identified network connections or associations.

[5] 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.

Category	Goal
Store	Able to store intrusion detection information for up to three years in a central database (a central database per site, and a central database at the federated level). The database should have sorting, querying, and backup capabilities. The database ideally will be a commercially available off-the-shelf system currently in use in the Air Force (e.g., Oracle 7).
Playback	Able to retrieve information from long-term storage and present it to an analyst. This capability should be such as to enable the analyst to review the sequence of networking events involved in an attack and to test new detection criteria against the sequence.

Architectural

The way the Air Force intends to do intrusion detection, as briefly described earlier in the operational overview, suggests several architectural goals. The tiered operation with centralized report gathering and correlation capability strongly suggests distributed capabilities. Architectural goals such as this, as well as others that take advantage of technology trends, are identified in this section using the following categories:

Physical Distribution: the physical locations of the intrusion detection capabilities

Functional Allocation: the allocation of intrusion detection functions to platforms, servers, other network resources, and intrusion detection servers

Distributed Control: the ability to remotely control dynamic configuring, detection focus, response patterns, and so forth

Network Protocols: the networking protocol suites the intrusion detection capability will be able to work with

Multitasking: the capability to perform more than one major task at a time, such as with background and foreground processing

Stealth: the ability to conduct intrusion detection operations without being detectable

Interoperability: the ability to work cooperatively with other networking capabilities such as network management systems

Platforms: the computers in which the intrusion detection system will be able to operate

Storage: the capacity to retain intrusion detection information for a period of time

Evolution: the ability to change to meet new requirements, to adapt to changing technologies, to conform to modified networking topologies, and so forth

Table 2 presents near-term architectural goals.

Table 2. Architectural Goals

Category	Goal
Physical Distribution	At the site level: Able to monitor network traffic from several locations within the network and able to collect intrusion detection information at several locations within the network.
Functional Allocation	The system should be modularly constructed to allow functional allocation suitable for the complexity and size of the network to be monitored. Thus, for a small network in which all traffic is visible from a single connected computer, it should be possible to operate all ID functions on a single platform. For larger networks where several vantage points may be necessary to monitor all traffic, it should be possible to allocate the monitoring function to several distributed platforms while operating the collection and storage function at a single central server. Similarly, the set of analysis functions should be partitionable across the monitoring systems and the central server.

Category	Goal
Distributed Control	Able to be reconfigured from one or more control locations. Distributed modules (such as monitoring modules, as described above) should have a control interface through which the control units of the system can provide reconfiguration and other commands for dynamically adjusting behavior. The system should allow for both networked and dial-in access to the control systems. Each control unit should be capable of operating independently of the others, even if connection to a central server (if any) is lost.
Network Protocols	At the site level[6] (e.g., on an intranet), network monitoring should be able to operate with at least TCP/IP protocol suite operating over Ethernet, Fast Ethernet, IEEE 802.3, and FDDI Microsoft Networking protocols operating over Ethernet, Fast Ethernet, IEEE 802.3, and FDDI Banyan Vines operating over Ethernet, Fast Ethernet, and IEEE 802.3 Novell Network operating over Ethernet, Fast Ethernet, and IEEE 802.3 At the federated level (e.g., on the Internet), network monitoring should be able to operate with TCP/IP traffic on ATM, X.25, and ISDN Novell traffic on ATM, X.25, and ISDN

[6] The network protocols used by deployed forces are the same as for fixed bases.

Category	Goal
Multitasking & Noninterference	At a central server, data analysis, collection, and monitoring functions should run in parallel. Distributed functional modules, such as monitoring modules, should run in parallel with other processing being done on their platforms. Control modules installed in client workstations should run in parallel with other client functions (e.g., word processing, email) when the client platform provides true multitasking. Moreover, the control module and any other intrusion detection software of the system installed on the client workstation should require no modifications to and should not interfere with the operation of client workstation applications software.
Stealth	The system should not be detectable as a network monitoring system and should have no noticeable effect on normal network operations, except insofar as it is required to perform intrusive, retaliatory actions.
Interoperability	The system should be interoperable with existing infrastructure components, such as IP routers, Certificate Authority platforms, Directory Services, Key Management Centers (KMCs), and Network Management Centers (NMCs).
Platforms	Client workstation intrusion detection software (e.g., control modules) should be able to interact with the current and next-generation versions of BSD, Solaris, Linux, OS/2, Windows 3.1, Windows 95, Windows NT, Next, and MacOS clients. The server software should run on the current and next-generation versions of Sun Microsystems' SPARC 5 and Ultra SPARC platforms running the Solaris 2.5 operating system and on Pentium or Pentium Pro PC running Windows NT and the Linux operating systems.

Category	Goal
Storage	At the federated level: All intrusion detection information should be storable at a central (single logical) database for analysis and long-term storage. The central database should provide data sorts and queries and should have backup capability. At the site level: All intrusion detection information should be storable at a central (single logical) database for analysis and forwarding to the federated central database.
Evolution	In general, the system should be modular, extensible, and upgradable. The tool should initially be feasibly deployable and its architecture should permit upgrading and growth in response to a changing technical environment. There should be a mechanism for easily updating detection algorithms as new penetration methods are discovered, or as operators define new requirements. It should be possible to easily incorporate new signatures that gain notoriety. The operator or administrator should be able to add new rules or policy to indicate what is or is not to be considered an intrusion. It should be possible to easily incorporate knowledge of new protocol services for purposes of network monitoring and analysis.

Human Interface

Experience with existing tools is the best teacher on needed improvements in the way intrusion detection capabilities can be managed and operated by a human. Our own experiences with tools (e.g., Intrusion Detection “Fly-Off” (G023 1997), testing at various operational military sites, and specific product testing (McBrien 1996(a))) as well as those of our sponsors, particularly the 609 IWS and the Air Force Information Warfare Center, indicate the desirability of a number of features identified in this section using the following categories:

Configurability: the ability to change detection focus and thresholds, response patterns, reporting and alarming behavior, and so forth

Ease of Use: characteristics of the human interface that contribute to the human's efficient use of the intrusion detection tool

Graphical Interface: characteristics of the human interface that provide pictorial information

Noninterference: the characteristic of operating unobtrusively and without noticeable performance degradation on a user's workstation

Table 3. Human Interface Goals

Category	Goal
Configurability	The system should be configurable to monitor traffic and not begin data collection until suspicious activity is detected. Alarms that announce detection should be operator configurable (e.g., set a level of concern such as *cautions*, *warnings,* and *alerts*). The system should be configurable to respond in real-time to a threatening behavior with a preconfigured response or to present a list of candidate responses to an administrator. For example, if an intrusion is detected on a critical server, the monitoring system could automatically end the session.
Ease of Use	The system's user interface should be intuitive and easy to use. Clear and extensive on-line help should be integrated with the administrator's and analyst's tools, including context-sensitive help wherever appropriate. The system should provide a "language" with simple semantics so that operators can add new "rules" or "policy" (specifying what is or is not an intrusion). The language should be robust enough to become a standard to be used at all AF sites with many different commercial products.

Category	Goal
Graphical Interface	The system's user interface should use graphical elements to enhance rapid human recognition and understanding of presented information; for example, a network map showing probable systems under a coordinated attack might be pictorially presented to enable rapid assessment of the geographical layout of the attack. The analyst's tool should be able to graphically display servers, routers, hubs, network status, and compromised or suspicious connections or hosts.
Noninterference	Any administrator or analyst tools that can reasonably operate in background mode should be transparent to the user to the extent possible.

Section 4

Implementation Goals

This section identifies goals related to the performance, maintenance, and use of intrusion detection tools in the categories

Efficiency

Maintenance

Security

Standards

Training

Efficiency

The intrusion detection system should conform to the temporal performance profile defined in the next table.

Table 4. Temporal Performance Goals

Function	Goal
Monitor, Detect, Capture, Control, and Collect	Perform in real time
Analyze	Perform current detection and assess state of network in near-real time Analysis of historical data has no performance-time constraint
React	Take predetermined action in real time Take administrator-selected action immediately upon selection
Notify	Activate alarm immediately upon recognizing the need for the alarm (Note: recognition might occur minutes or hours after event as a result of background analysis)
Report	Provide requested information within 30 seconds of request
Store	Store data for up to three years
Playback	Provide requested information within 5 minutes of request

The system should be capable of continuous operation 24 hours a day, 7 days a week.

Maintenance

The system should provide integrity checking mechanisms to detect whether modifications have been made to critical configuration and data files as well as the system's software. Examples of such mechanisms include integrity checksums, such as those provided by Tripwire. The system should provide self-test (e.g., on startup, periodic.) employing the integrity checking mechanism to ensure that it itself is in a correct state for operation (e.g., code has not been modified, configuration files have not been changed).

Security

Protecting Control Information and Data — Since operational security is an issue, all data and control traffic to and from the site systems and the central server at the federated level should be protected from threats to confidentiality, integrity, and availability (e.g., by encrypting to the Sensitive But Unclassified (SBU) level). The protection scheme should be designed to operate without operator (i.e., administrator or analyst) intervention. In addition, the system should be able to operate with encryption hardware that meets DoD security standards for the transmission of classified information when monitoring classified systems.

Certification of the Monitoring Systems — System components monitoring classified, including SCI, networks should be certifiable for system-high operation with appropriate physical security.

Protection of the System Components — All system components (monitors, control agents, servers) should be constructed and configured to prevent unauthorized access to data, unauthorized modification of databases, data files, and software, unauthorized resource usage, and unauthorized reconfiguring or rebooting whether locally initiated or remotely initiated from another network location.

Standards

Where applicable, the system should be based on existing standards or should be evolvable to a standards-based tool.

Training

Training should be provided for using each component of the tool. Besides whatever training methods a vendor may consider suitable, training should also be available in the form of one or more student-paced, automated tutorials, for use in situations where other media may not be available or appropriate. This training should be adequate to enable users to use all basic capabilities of the tool with confidence. In addition, appropriate on-line help,

including context-sensitive help where that makes sense, should be available for all components of the tool.

List of References

AFCERT 92 AFCERT, *Air Force Computer Emergency Response Team: Concept of Operations (CONOP)*, AFCERT Working Note, not in the public domain.

AFIWC 96 AFIWC, December 1996, *Requirements Document for an Automated Global Intrusion Detection System.*, not in the public domain.

G023, 1997, Network Monitoring and Intrusion Detection "Fly-Off", ongoing effort described in unpublished PowerPoint document, The MITRE Corporation, McLean, Virginia, not in the public domain.

McBrien, Andrew, September 1996, *Results of Intrusion Detection Product Testing for 609 IWS*, unpublished MITRE Working Note, The MITRE Corporation, Bedford, Massachusetts, not in the public domain.

McBrien, Andrew, September 1996, Appendix "609 IWS Network Monitoring System Requirement" in unpublished MITRE Working Note *Results of Intrusion Detection Product Testing for 609 IWS*, The MITRE Corporation, Bedford, Massachusetts, not in the public domain.

Sandia National Laboratory, October 1996, *National Info-Sec Technical Baseline: Intrusion Detection and Response*, URL: http://doe-is.llnl.gov/nitb/docs/nitb.html, Lawrence Livermore National Laboratory, Sandia National Laboratory.

Appendix

An Abstract Intrusion Detection Architecture

The idealized architecture described here is based on the goals in this paper, some design ideas being used in the CyberCops[7] MOIE project, sponsored by the Army, and the concept of operation for the Air Force Computer Emergency Response Team (AFCERT 92).

Figure A-1 depicts the site level components of an intrusion detection architecture that might satisfy the functional and architectural goals identified in the body of this paper. This picture shows elements at several levels within the protection domain. Parts of an intrusion detection capability that would be added to existing systems (e.g., workstations, servers, routers) are shown as ID add-ons. New components are depicted as ID Control elements: these components perform the storage, analysis, reporting, and control functions.

The ID add-ons represent all the intrusion detection functions needed for the platforms on which they are installed. The functional goals for these add-ons are beyond the scope of this paper; the control functions within these add-ons are those needed to realize the architectural goals and are within the scope of goals in this paper.

Figure A-2 depicts the intrusion detection architecture at the federated or global level. The Federated Intrusion Detection System provides the ability to correlate various incidents to develop an overall attack-response posture.

[7] This MITRE project is developing an electronic police force that will protect networked computer systems from electronic attacks. The electronic police force will have the following responsibilities: (1) collect and maintain information on vulnerabilities, threats, and risk levels; this information can be used to prevent electronic attacks; (2) detect electronic attacks in real-time; and (3) respond to electronic attacks; for instance, identify electronic attackers, limit damage, and analyze code and data left behind from attacks.

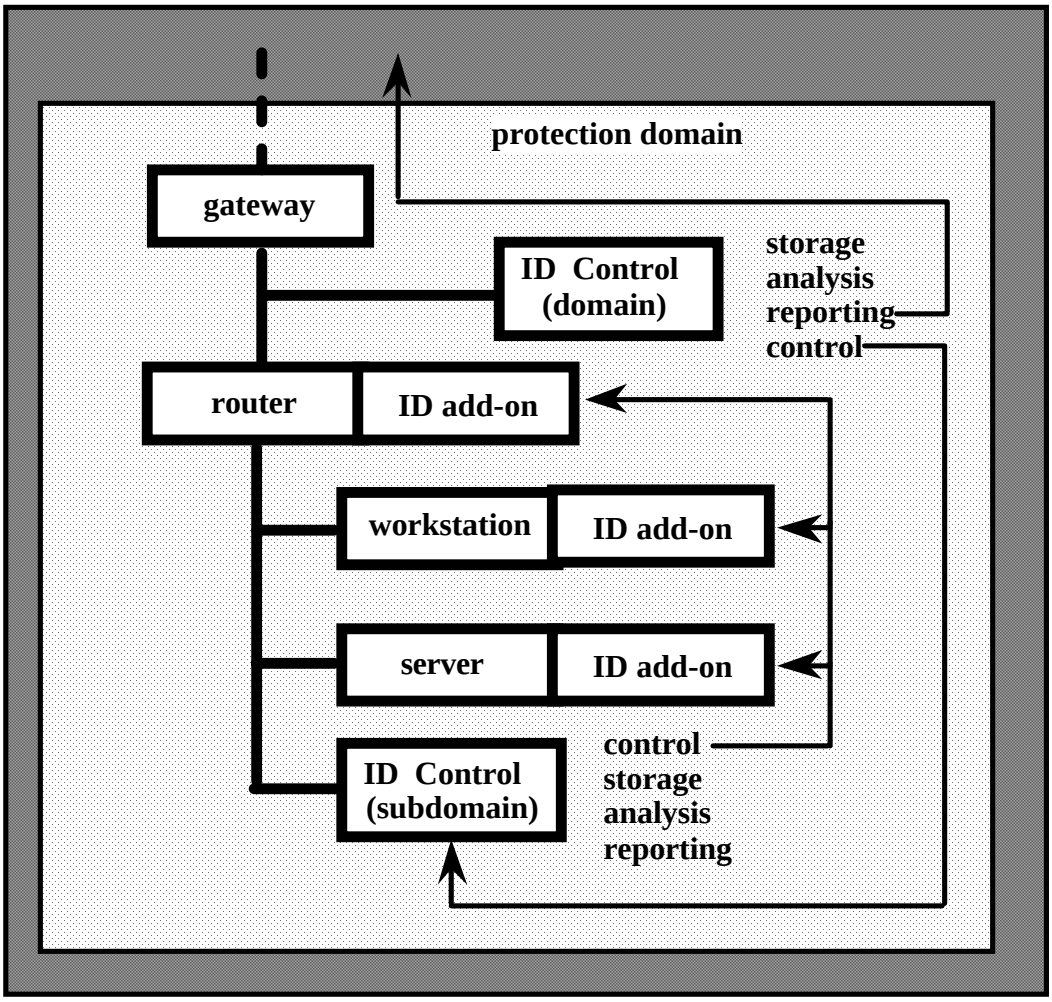

Figure A-1. An Intrusion Detection Architecture: Site Level

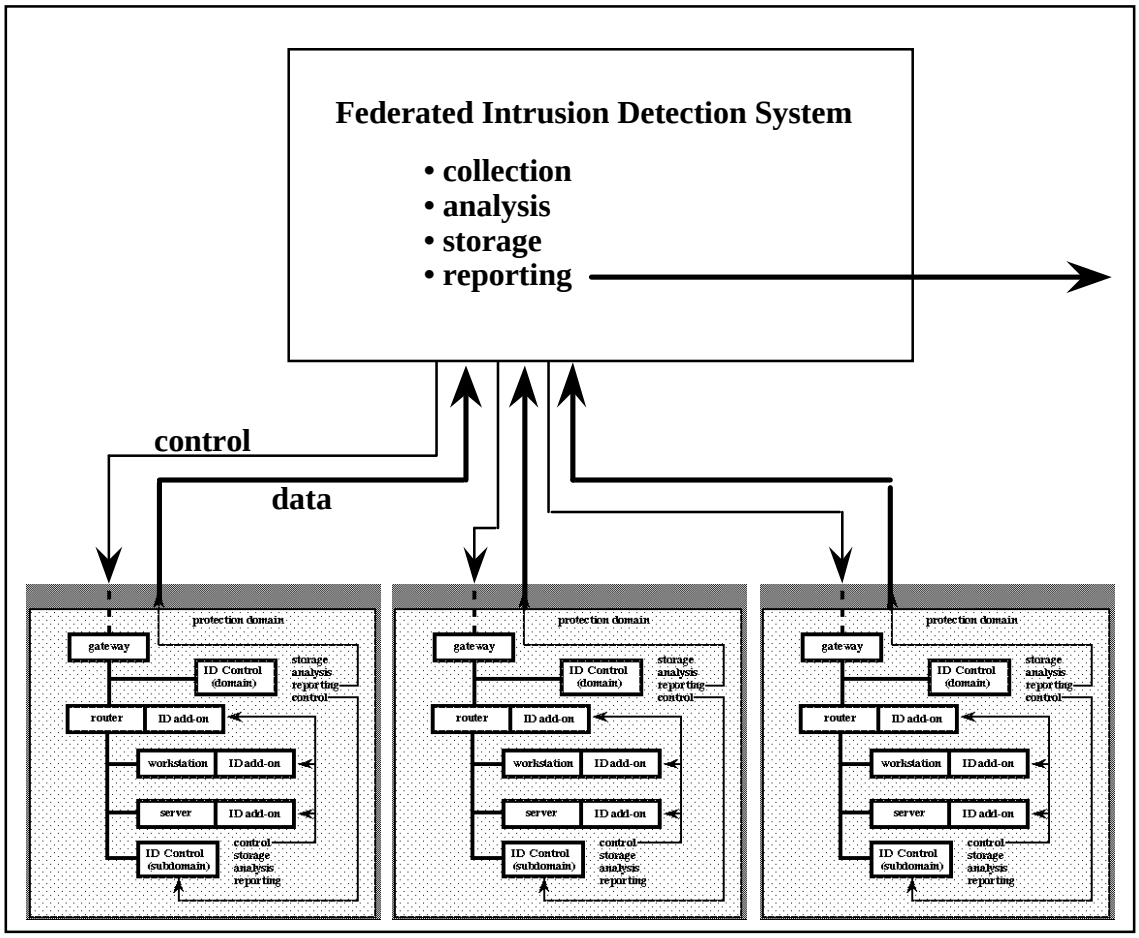

Figure A-2. An Intrusion Detection Architecture: Federated Level