MTR 98B0000066

MITRE TECHNICAL REPORT

Intrusion Reaction

Recommendations for Obtaining Reaction Capabilities

September 1998

Leonard J. LaPadula

Sponsor: Air Force
Dept. No.: G021

Contract No.: F19628-94-C-0001
Project No.: 039874520B

Approved for Public Release: Distribution Unlimited.
03-0414

© 1998 The MITRE Corporation. All rights reserved.

MITRE
Center for Integrated Intelligence Systems
Bedford, Massachusetts

MITRE Department Approval:

Dr. Marion C. Michaud
Department Head
Information Warfare and Secure
Systems Engineering

MITRE Project Approval:

Michelle J. Gosselin
Project Leader, 03987452

Abstract

The Command and Control (C2) Protect Mission-Oriented Investigation & Experimentation (MOIE) Project, sponsored by the Air Force, develops and promulgates resources to counter information warfare (IW) threats to military C2 computer networks. This report has been produced by the Intrusion Reaction task of the project.

A growing threat to Air Force networks and computers is exploitative intrusion activity. One technological countermeasure to exploitative intrusion activity is intrusion reaction capability. But intrusion detection and reaction (IDR) systems in operation today do not provide a number of reaction features that might materially help the Air Force protect its networks and computers. This report develops a profile of such features. It recommends areas where the Air Force can make effective investments in research, development, and investigation of intrusion reaction capabilities that can improve IDR systems.

KEYWORDS: Information Protection, Intrusion Detection and Reaction, Intrusion Reaction, Recommendations

This Page Intentionally Left Blank

Executive Summary

The intrusion detection and reaction (IDR) systems in operation today fall far short of ideal capability to react to intrusions. This report recommends areas for effective Air Force investments in research, development, and investigation of reaction capabilities for defensive intrusion detection and reaction (IDR) systems.

To develop our recommendations we compare the state of the art to an ideal set of capabilities. We base our ideal on our understanding of Air Force networks and current defensive information operations.

In light of our review of pertinent facts and circumstances, we recommend that the Air Force research techniques and develop capabilities in three important areas where we do not expect commercial coverage over the next several years. They are

- Analysis, Investigation, and Decision Support
- Vulnerability Management
- Damage Management

We also recommend that the Air Force

- Encourage vendors to enhance their products by adding capabilities in these categories
  - Developing Forensic and Other Data
  - Domain Adjustment[1]
  - Information Collection
  - Self-adjustment[2]
- Encourage vendors to improve their products in their ability to provide alerts by developing capability to
  - Correlate possible attacks
  - Discover unresolved attacks by review of logs

---

1 The IDR system, working cooperatively with other components in the domain of protection such as routers and firewalls, can adjust security policies, filtering policies, configuration parameters, permissions, and so forth.

2 This refers to capabilities to adjust the way the IDR system behaves or to adjust parameters of operation to correct or improve them. Examples are adjustments to detectors to reduce false alarming, resetting event auditing, and changing the audit-events to be logged.

Finally, we recommend that the Air Force foster development of auxiliary capabilities identified in our analysis, placing special emphasis on

- Government-developed attack-response criteria, damage-reporting criteria, and recovery-priority criteria
- An IDR command, control, and reporting messaging system, including protocol and message format standard, to enable inter- and intra-IDR system communications
- One or more standards specifying content and format for entries in logs, history files, and so forth to facilitate exchange of information among IDR systems

Acknowledgments

I thank Marion Michaud, Department Head, and Michelle Gosselin, Section Leader and C2 Protect MOIE Task Leader, both of MITRE G021, for their encouragement, leads to sources of information, and helpful comments on the final draft of this document.

I thank Cal Norton, Information Analyst, MITRE R103, for her information searches on my behalf that turned up relevant, useful sources of information.

Special thanks to Steve Godin who, drawing on his work experience with preparation of forensic data, provided helpful guidance to me in this area.

This Page Intentionally Left Blank

Table of Contents

Section	Page
Introduction	**1**
Purpose and Scope of this Report	1
Approach	1
Compendium of Desirable Reactions	**3**
Introduction	3
Detection in Real Time	5
Reactions for a Verified Attack	5
Dealing with the Intrusion	5
Dealing with the Effects of an Intrusion	7
Dealing with the Vulnerabilities that Allowed the Attack to Succeed	7
Take Actions that Assist in Dealing with the Intruder	7
Reactions for a Possible Attack	8
Reactions for a False Alarm	8
Detection during Analysis of Logs	9
Summary	9
Summary of the State of the Art in Intrusion Reaction	**13**
IDR Capabilities for Investment	**17**
List of References	**21**
Appendix Reactions, Files, and Definitions for Compendium of Reactions	**23**
Distribution List	**29**

List of Figures

Figure		Page
1	IDR Units Deployed in a Local Area Network	4

List of Tables

Table		Page
1	IDR System Reactions Organized by Category	9
2	Reactions Provided by COTS IDR Products	17

Section 1

Introduction

The Command and Control (C2) Protect Mission-Oriented Investigation & Experimentation (MOIE) Project, sponsored by the Air Force, develops and promulgates resources to counter information warfare (IW) threats to military C2 computer networks. One kind of threat is exploitative intrusion activity, which appears to become more serious every day. Given the missions executed using Air Force C2 systems, the rewards of a successful IW attack on our C2 systems invite the attempt at exploitation. Since military systems may be connected to and dependent on public switched networks, they can be accessed for exploitation. Moreover, we know that many of our C2 systems are vulnerable from investigations performed by Air Force Information Warfare Center (AFIWC), Electronic Systems Center (ESC), Defense Information Systems Agency (DISA), Fleet Information Warfare Center (FIWC), MITRE, and others.

Purpose and Scope of this Report

One technological countermeasure to exploitative intrusion activity is intrusion reaction capability. When attacks are detected or suspected, many defensive actions might be carried out that can thwart attackers' intentions. The intrusion detection and reaction (IDR) systems in operation today fall far short of ideal operational capability. This report provides a planning tool for Air Force use, to assist in making effective investments in research, development, and investigation of intrusion reaction capabilities for intrusion detection and reaction (IDR) systems.

In this report, we assume that the reaction system is a defensive reaction system. In identifying possible reactions we limit our consideration to defensive reactions and only indicate places where the defensive system might provide information to an offensive IW unit.

Approach

We develop a compendium of possible reactions to detected anomalies, in the form of an operational classification. The operational classification identifies a reaction for each case that can arise. Cases for consideration are systematically generated by logical analysis. Next, we summarize the state of the art in reaction systems. Finally, by comparing the compendium to the state of the art, we develop a picture of the functional and technological landscape, identifying promising areas for Air Force investment.

In short, the report describes an ideal, compares the state of the art to it, and identifies reaction capabilities for the Air Force to research, develop, or foster.

This Page Intentionally Left Blank

Section 2

Compendium of Desirable Reactions

In this section, we develop a compendium of possible reactions for an IDR system. We develop the compendium by identifying desirable reactions to detection of an anomaly in a computer or network. This provides an operational classification of reactions by systematic consideration of relevant cases.

Introduction

We imagine that the (IDR) system we are talking about is patterned on the model of the notional architecture described in the CyberStrike Roadmap [1]. In that architecture, there are three kinds of IDR units.

- IDR Sensor**:** An IDR Sensor is a software/hardware component that one adds to a system such as a server or workstation to provide intrusion detection and reaction functions specific to that system. An IDR Sensor can operate independently of other IDR capabilities to protect the system on which it is installed. It may also provide exported data or reports that can be used by other IDR capabilities.
- IDR Agent**:** An IDR Agent is a software/hardware component that one adds to a system such as a router to provide intrusion detection and reaction functions specific to the domain of the IDR Director on whose behalf it operates. An IDR Agent is designed to work cooperatively with an IDR Director.
- IDR Director**:** An IDR Director is a software application or a software and hardware ensemble that performs storage, analysis, reporting, and command/control functions. It can be implemented on a stand-alone system or it can share a platform with other applications**,** running "independently" of the system on which it is installed, such as a server that hosts several different functions. An IDR Director controls the IDR Agents and may interact with IDR Sensors within its domain.

Figure 1 shows the units as they might be deployed in a local area network.

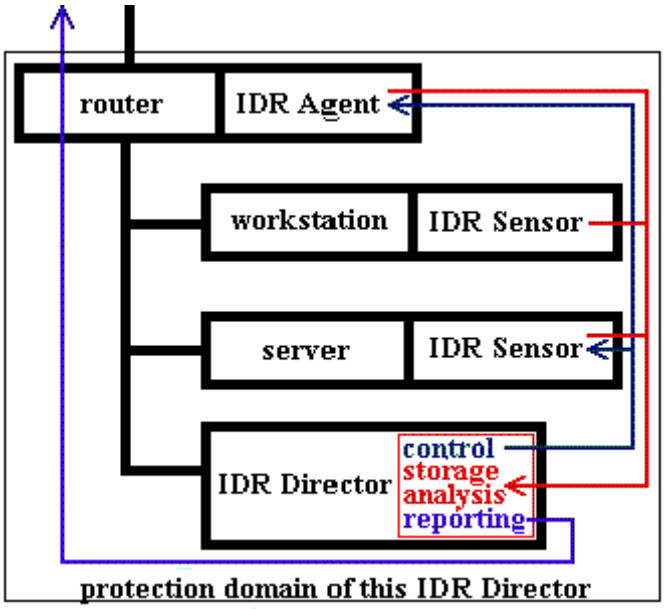

Figure 1. IDR Units Deployed in a Local Area Network

We develop the operational classification for a complete IDR system, which includes multiple Sensors and Agents, at least one Director, and IDR personnel. The Sensor units are assumed to be doing both host-based and network-based intrusion detection in real time.

We will not generally identify which type of unit performs the reactions listed below, or even whether the reactions are done by automated means or by IDR personnel. Many implementations are possible. In general, we would want as much as feasible done by automated means since personnel with appropriate skill levels are scarce [2]. Some reactions are clearly doable only by a human, some are more suited to a Director unit than a Sensor unit, or vice versa. Assigning responsibility for a reaction in some cases may be determined solely by considerations of implementation.

In describing the reactions, we will not mention that a reaction should be performed if it is feasible. The reader should understand that this condition applies to all reactions.

Reactions in the operational classification that follows are actions triggered by the detection of an anomaly. An anomaly may occur because of an intrusion attempt or because of a condition or malfunction internal to the system being monitored. Since the scope of this report is limited to examining intrusion reactions, we take account of other anomalies only to the extent of distinguishing them from an intrusion attempt.

We consider reactions in two cases—detection occurs in real time and detection occurs during analysis of logs.

Detection in Real Time

When an anomaly or suspicious event is noticed, the reaction system performs triage. Triage may classify the suspicious event as

- Internal Fault[3]
- Verified Attack
- Possible Attack
- False Alarm

Reactions for a Verified Attack

The reaction system does four things[4] related to the intrusion:

- Deal with the intrusion
- Deal with the effects of the intrusion
- Deal with the vulnerabilities that allowed the attack to succeed
- Take actions that assist in dealing with the intruder

Dealing with the Intrusion

The IDR system logs the event in a History of Incidents file. This file can be used subsequently either locally or at a higher level in combination with History of Incidents files from other IDR systems. Analysis and investigation of the information recorded in these files can produce histograms, identify trends, help discover methods of attack, and assist in identifying the source of an attack.

The reaction system first determines whether the attack should be shut (if possible) or monitored. To do this it needs guidelines, which we might call attack-response criteria. The

---

[3] Given the scope of this report, we do not consider reactions to internal faults in the operational classification. However, there is no technological reason to limit the functionality of an IDR system to *intrusion* detection and reaction. More generally, we might consider anomaly detection and reaction (ADR) systems. Checking for errors of omission, misconfigured applications, improperly implemented policies, as in firewalls, and errors in system configurations are just a few examples of what could be done, in addition to intrusion detection, by an ADR system. One might even argue that internal faults give rise to more difficulties in automated systems than do intrusions.

[4] To the extent possible, these jobs would proceed in parallel.

criteria are based on factors such as criticality of the system, nature of the attack, and effect on the system. For example, the reaction in an operationally critical system that is only slightly performance-impaired by the attack might be to shut the attack on the assumption that *any* performance degradation will impair mission execution. The reaction in an administrative system might be to monitor the attack although the system is severely performance-impaired. Delaying completion of its administrative functions might be permissible. Monitoring the attack may yield useful information to prevent or deter future attacks, may provide information helpful to an offensive IW unit, or may enable collection of forensic data.

Shutting the Attack. In some cases, shutting the attack is easy. TCP[5] connections, for example, can easily be terminated. Other attacks cannot always be shut off by the system experiencing the attack. A workstation being flooded with UDP[6] packets is dependent on a router or other network component for stopping the attack. Thus, shutting the attack may involve communication between the attacked system and a network component. In the architecture depicted earlier, a Sensor would send a message to the authorized Director, informing it about the attack it is experiencing. The Director would send a message to its Agent located in the router, directing it to block the attacking packets.

A situation such as just described may pertain on a larger scale. It may be that the IDR system cannot shut off an attack originating outside its protection domain. In this case, the Director would send a message to the Director at the next higher echelon of protection.

Monitoring the Attack. In some cases, monitoring can be performed by the system experiencing the attack. However, monitoring could be performed by a system other than the one being attacked. For example, suppose a workstation is being attacked via a TCP connection. In the architecture depicted earlier, the IDR Sensor in the workstation (see Figure 1) could report the attack to the Director unit. The Director could send a command to an agent in another workstation (not depicted in Figure 1) to take over the connection (hijack) and collect forensic data. When there is a connection between the attacker and the monitoring system, monitoring can use manipulation[7] of the connection. Manipulation may reveal the source of the attack or yield forensic data.

---

5 Transport Control Protocol

6 User Datagram Protocol

7 In this context, connection between the attacker and the monitor simply means that the monitor is able to send data to the attacker as a normal part of whatever it is that the attacker is doing. This is easy to see in the case of a TCP connection that is being used by the attacker. For example, the monitor might intentionally send ACK (acknowledgment) packets with out-of-sequence numbers.

When there is a connection between the attacker and the monitoring system, monitoring can use manipulation of the connection.

Dealing with the Effects of an Intrusion

For dealing with the effects of the intrusion, the reaction subsystem does the following:

- Log intrusion in a history of incidents file
- Assess the damage
- Decide whether to report the damage
- Determine whether operation can continue
- Determine recovery priority
- Carry out recovery actions
- Make adjustments to automated elements within the protection domain

To find the effects of an intrusion the IDR system might look at system logs, history logs, and other logs produced by the IDR system, a router, a firewall, and so forth. It can look for hidden data, such as a user file stored in a system directory on a UNIX system. The IDR system can perform integrity checks: it might compare a computed MD5 checksum for a file to a prestored MD5 checksum for that file. It can search for bad files such as known malicious programs and viruses.

Dealing with the Vulnerabilities that Allowed the Attack to Succeed

The vulnerability that the attack exploited could involve systems other than the one attacked. For example, it is conceivable that an attack on a workstation succeeded because of a failure in a firewall system within its protection domain. A workstation that detects loss of service may be the victim of an attack on a router that serves its subnetwork. The reaction system carries out the following reactions:

- Determine which system has a vulnerability that allowed the attack to succeed
- Determine what the vulnerability is
- Discover whether the IDR system has a remedy for the vulnerability
- Determine whether the remedy can be applied to the system
- Apply the remedy to the system

Each reaction in the preceding list is dependent on the success of the prior reactions.

Take Actions that Assist in Dealing with the Intruder

The scope of this report is limited to defensive IDR systems. Thus, we consider only passive actions that might assist an offensive IW unit or a court of law in dealing with the intruder.

The defensive IDR system can report intrusions to an appropriate offensive IW unit. The report can include information about the intrusion that might assist in discovering the source of the attack, the location of the intruder, the intention of the intruder, the methods of the intruder, and so forth.

The defensive IDR system can gather forensic data that might assist in prosecuting an attacker. It can collect data to be evaluated by law enforcement as possible evidence. This data might be used to establish the method and time of the attack, the damage caused by the attack, the cyber and possibly the physical source of the attack, the identity of the attacker, and so forth. According to Godin, looking at this from a law-enforcement perspective suggests that the IDR system should take these steps in preparing forensic data [3]:

1. Locate data for evaluation as evidence.
2. Preserve the data: the original data must be preserved in case the defense wishes to see the data in its original state or conduct forensic analysis on the data in their own manner.
3. Copy the data for forensic analysis. An image of potentially evidential data is made and the forensic analysis is done on the image. If the data and analysis were brought into court, a law-enforcement officer likely would testify to the validity of the copy and the forensic analysis. If something untoward were to occur, the original data would still be available.

To preserve the data collected for evaluation, the IDR system can store the data in a manner that ensures its integrity. For example, the container of the data can be date-time stamped and sealed cryptographically to enable authentication and prevent tampering.

Reactions for a Possible Attack

The IDR system tries to resolve the anomaly that triage has classified as a possible attack. The IDR system

- Logs the possible attack in a Possible Attacks file
- Monitors the anomalous circumstances
- Correlates the anomaly with other possible attacks and reports or alerts, as appropriate

Reactions for a False Alarm

The IDR system does what it can to reduce false alarming. It might dispatch an Agent to change a policy or send a command to a Sensor to change its settings. The IDR system

- Logs the false alarm in a False Alarms file
- Adjusts detection to reduce false alarming

Detection during Analysis of Logs

Analysis of logs can do more than detect intrusions. It can also find internal faults. A Director unit analyzing logs of its Sensors may be able to tell that a workstation has a misconfigured Registry. The Sensor that reported the data in the log might not have been able to make the determination. It might simply not have been programmed to do so or it might not have been able to acquire auxiliary information needed to do the analysis. Detection of internal faults in this way gives rise to a number of additional functions for an ADR system, which are beyond the scope of this report. We deal here only with the follow-up to detection of intrusions.

When the IDR system discovers an anomaly that is not an internal fault, it

- Determines whether the investigatively discovered intrusion has already been resolved
- Notifies IDR personnel for attacked system about an unresolved intrusion

Summary

This compendium of desirable reactions has identified many defensive reactions that might profitably be implemented in an IDR system. Table 1 lists the reactions, organized by categories. The appendix describes each of the reactions, describes files referenced in the descriptions of the reactions, and provides definitions of some key terms.

Table 1. IDR System Reactions Organized by Category

Category	Reaction
Alerting	Notify IDR personnel or other automated elements of the IDR system about an attack, a correlated possible attack, or a hitherto unresolved attack discovered investigatively by review of logs
Analysis, investigation, and decision support	Perform triage Review incident logs Decide whether damage should be reported Determine whether operation of the system can continue Determine recovery priority Determine which system has a vulnerability that enabled the attack Determine what the vulnerability is Correlate a possible attack with other possible attacks Determine whether an investigatively discovered intrusion has already been resolved

Category	Reaction
Attack management	Shut attack Monitor attack Monitor anomalous circumstances
Damage management	Assess damage Prioritize recovery Carry out recovery action
Developing forensic and other data	Collect relevant data Manipulate a connection
Domain adjustment	Make adjustments to automated elements within protection domain
Information collection	Log intrusion in History of Incidents file Log possible attacks in a Possible Attacks file Log false alarms in a False Alarms file
Self-adjustment	Adjust detection to reduce false alarming
Vulnerability management	Determine what the vulnerability is Determine which system has a vulnerability Discover whether the IDR system has a remedy for the vulnerability Determine whether a remedy can be applied to a system Apply a remedy for a vulnerability

In developing the operational classification, we have identified a need for the following auxiliary components or properties of an IDR system:

- History of Incidents file
- Possible Attacks file
- False Alarms file
- Attack-response criteria
- Damage-reporting criteria
- Recovery-priority criteria
- An IDR command, control, and reporting messaging system, including protocol and message format standard, to enable inter- and intra-IDR system communications
- One or more standards specifying content and format for entries in logs, history files, and so forth to facilitate exchange of information among IDR systems

- A collection of tools that can be launched by the reaction systems and whose results can be used by the reaction system (for example, vulnerability scanning tools)
- A database or file of remedies for vulnerabilities
- A method for sealing data with a date-time stamp in a manner that enables authentication and prevents tampering
- Potentially extensive storage and retrieval capacity

This Page Intentionally Left Blank

Section 3

Summary of the State of the Art in Intrusion Reaction

Commercially available intrusion detection products generally implement one or more of the following reaction capabilities:

- Terminate: The intrusion detector terminates the session (for example, TCP connection) of the suspected attack.
- Log: The intrusion detector logs the suspicious event.
- Record: The intrusion detector records the sequence of data units (for example, packets) involved in the suspected attack and saves them for later playback or analysis.
- E-mail: The intrusion detector sends e-mail to a designated operator or administrator describing the suspected attack.
- Page: The intrusion detector pages a designated operator or administrator to indicate that suspicious attack has been detected.
- Capture: The intrusion detector alerts an administrator in real time and the administrator takes over the session[8] (for example, TCP connection) of the suspicious activity

The emphasis in commercially available products is on detection. The reaction capabilities listed above provide little more than connection termination, alerts, and logging. A recent study by the President's National Security Telecommunications Advisory Committee noted the apparent lack of automated damage assessment and response: [4]

> "Although IDSs are readily available for alerting organizations that they are being attacked, no systems appeared to provide them with an automated damage assessment and response capability. Advanced damage assessment and response tools could provide organizations with an ability to determine the extent of an intrusion and its potential impact on the network."

The National Info-Sec Technical Baseline report noted the same deficiency in its 1996 survey, claiming that Damage assessment and recovery mechanisms are lacking in the vast majority of systems [5].

---

[8] We have not seen any claims that the intrusion detection and reaction software automatically captures a session.

It also identified these practical issues

- Testing is lacking, with most systems rarely tested beyond demonstrating that they detect some anomalous events
- Scalability: To be of significant utility in modern information environments, IDR systems must be capable of handling large numbers of events. In contrast, most of the systems examined by the reporters detect events at the system level. Work directed toward correlating activity between systems is in the very early stages and much more work needs to be done.

The report stresses the importance of identifying the source of an attack and states that traceback capability is most difficult in the computer-networking environment.

The state of the art for network-based intrusion detection was described in September 1997 by Hill and Aguirre [6]. Among their findings, the following points are relevant to intrusion reaction:

- Better analysis support is an urgent need:
  - Improved expert systems should reduce the false alarm rate
  - Better distribution of problem identification is needed
  - Tools that can correlate activity from distributed sources and activity directed toward distributed targets are crucial to address issues of information warfare.
- There is growing recognition that there would be high utility in integrating the output of different entities involved in network security, including routers, firewalls, proxies, and host-based and network-based IDSs.

For this summary, we reviewed 20 commercial off-the-shelf (COTS) products[9], several of them recent entries into the field, to compile a list of the responses they implement. Many of the 20 products provide the following responses:

- Notification to human via console message, e-mail, or pager
- Disable account
- Terminate access or log off the user
- Terminate session
- Terminate process

---

[9] AuditGuard 1.0, AutoSecure, Computer Misuse Detection System (CMDS™), Cybercop Scanner 2.4, ENTRAX, Flight Jacket 1.6.2, INTOUCH INSA Network Security Agent, IP-Watcher®, Kane Security Monitor 3.1, NetRanger, OmniGuard/ITA (InTruderAlert), POLYCENTER™ Security Intrusion Detector, PRéCis, RealSecure™, SecureNet Pro, Session Wall-3, Stake Out™, Stalker, Tripware IDS 1.5, and WebBoy

- Shut down the system
- Log user activity

Several of the surveyed products provide the following:

- Record the event on a security server
- Send alert to associated Director unit
- Execute a predetermined procedure[10]
- Provide reports giving summary, trending, or alert data

Each of the following responses is provided by only one or two products (no one product provides all)

- Hijack connection
- Store intrusion data in a relational database for subsequent analysis
- Limited self-adjustment after attack (reset event auditing, re-enable audit data generation)
- Reconfigure a Check Point Firewall-1 or Lucent Managed Firewall to reject traffic from the attacking source address
- Send an SNMP[11] trap to an SNMP compliant network management system
- Repair damaged files[12]

While we note the limited reaction capabilities present in COTS products, we should also recognize the difficulty for vendors to provide sophisticated capabilities in this area. To provide a useful automated response system, which could react intelligently in the context of the domain being protected, the vendor would have to build a system with significant built-in knowledge or a very capable knowledge-acquisition subsystem. For example, the system would have to know the information assets in its protection domain, their relative criticality to the mission, and their available modes of operation. It would have to know the policy for managing those assets under attack. The investment needed to create such a system may be

---

[10] Presumably, this provides a way for the user of the product to implement new capabilities such as for damage assessment and recovery.

[11] Simple Network Management Protocol

[12] This capability is claimed for Stalker 3.0 by Trusted Information Systems in a 1998 press release, at http://www.tis.com/corporate/press/98/stalker3pr.html (as of October 6, 1998).

more than a vendor is willing to risk on speculation[13]. In a commercial marketplace where enterprises are willing to buy relatively simple detectors, vendors may lack motivation to invest in research and development in this area.

Historically, capability to do more than detection and simple response has been developed by the government. Government off-the-shelf (GOTS) products and a number of government-sponsored research and development efforts are the result today. Two examples are Automated Security Incident Measurement (ASIM) and Intruder Detection and Isolation Protocol (IDIP). ASIM provides deployed detectors, widely distributed geographically, with a centralized analysis and notification system. IDIP, part of the DARPA[14]-funded research on Dynamic, Cooperating Boundary Controllers, is developing capability for interaction between the detector and a firewall to allow dynamic changes to firewall policy based on intrusion alerts.

The Air Force continues, necessarily, to investigate and develop IDR that can serve its needs not only to detect intrusions but also to manage its information assets within its domain of protection. To do so effectively requires that the IDR system have sophisticated ability to use and maintain databases of relevant information such as network map and vulnerability data. It uses this auxiliary information to produce analyses of various kinds to provide corrective feedback down to the level of the sensors.

The principal Air Force-developed system that demonstrates capabilities along these lines is ASIM. The two Air Force-sponsored research and development efforts exploring such capabilities are Extensible Prototype for Information Command and Control (EPIC[2)] and Spitfire [7]. In addition, AFIWC is upgrading the resources available to the AFCERT[15] along similar lines, the Oracle database capability being a prime example.

---

[13] The National Security Telecommunications Advisory Committee, Network Group, Intrusion Detection Subgroup stated in its report [3]: "Because national security and defense programs represent a shrinking market, industry is not willing or able to spend its limited R&D funds on high-risk and limited use technologies. The Government remains the only entity with the resources to invest in those high-risk R&D initiatives."

[14] Defense Advanced Research Projects Agency

[15] Air Force Computer Emergency Response Team

Section 4

IDR Capabilities for Investment

This section identifies capabilities of an IDR system that are not apparently present in today's COTS and GOTS products. They constitute the promising areas to investigate, in which to develop capability, or in which to foster research and development.

Comparing the compendium in this report to today's state of the art in intrusion reaction suggests that most categories of reaction need development. The categories best covered by COTS products are Alerting and Attack Management. The main additional category addressed by Air Force GOTS products is Analysis, Investigation, and Decision Support.

Table 2 indicates which categories of reactions in the compendium of this report are addressed by COTS products. Reactions provided by COTS products are highlighted in the table.

Table 2. Reactions Provided by COTS IDR Products

Category	Reaction
Alerting	Notify IDR personnel or other automated elements of the IDR system about an attack (using e-mail, paging, console message, message to Director unit), a correlated possible attack, or a hitherto unresolved attack discovered investigatively by review of logs
Analysis, Investigation, and Decision Support	Perform triage Review incident logs Decide whether damage should be reported Determine whether operation of the system can continue Determine recovery priority Correlate a possible attack with other possible attacks Determine whether an investigatively discovered intrusion has already been resolved
Attack management	Shut attack (methods reported include disabling an account, terminating access, logging off the user, terminating the session, terminating the process, and shutting down the system) Monitor attack (by recording sequence of data units such as packets or recording user activity) Monitor anomalous circumstances

Category	Reaction
Damage management	Assess damage Prioritize recovery Carry out recovery action (reset event auditing, re-enable audit data generation, repair damaged files
Developing forensic and other data	Collecting relevant data Manipulating a connection (by hijacking)
Domain adjustment	Make adjustments to automated elements within protection domain (reconfigure a Check Point Firewall-1 or Lucent Managed Firewall to reject traffic from the attacking source address, send an SNMP trap to an SNMP compliant network management system)
Information collection	Log intrusion in History of Incidents file Log possible attacks in a Possible Attacks file Log false alarms in a False Alarms file
Self-adjustment	Adjust detection to reduce false alarming
Vulnerability management	Determine What the Vulnerability Is Determine Which System Has a Vulnerability Discover Whether The IDR System Has A Remedy For The Vulnerability Determine whether a remedy can be applied to a system Apply a remedy for a vulnerability

In addition, some COTS products provide the following features that can be used to supplement the reaction capability of the product:

- Execute a predetermined procedure
- Provide reports giving summary, trending, or alert data
- Store intrusion data in a relational database for subsequent analysis

Reactions in two important categories appear to be absent in COTS products presently—the category Analysis, Investigation, and Decision Support and the category Vulnerability Management. It is noteworthy that the Air Force has some capability or has done some exploratory work in each of these areas. Investigative capability is evident in the operations of AFCERT personnel using the products of the ASIM system. Exploratory work in vulnerability management has been sponsored by AFIWC [8]. This exploratory effort used

the Security Tools & Vulnerability Database (STVDB) produced by MITRE, Rome, NY, under joint sponsorship of Air Force Research Laboratory and Army Research Laboratory.

Another important category of reactions where very little has been done in both COTS products and by the Air Force is Damage Management. Both national-level studies of intrusion detection and reaction stress the importance of damage assessment and recovery [3, 4].

In light of our review of pertinent facts and circumstances, we recommend that the Air Force research techniques and develop capabilities in these three important areas

- Analysis, Investigation, and Decision Support
- Vulnerability Management
- Damage Management

We do not expect capabilities in these areas to be forthcoming in COTS products over the next several years. The Air Force should

- Encourage vendors to enhance their products by adding capabilities in these categories
  - Developing Forensic and Other Data
  - Domain Adjustment
  - Information Collection
  - Self-adjustment
- Encourage vendors to improve their products in the Alerting category by developing capability to
  - Correlate possible attacks
  - Discover unresolved attacks by review of logs

Finally, we recommend that the Air Force foster development of the auxiliary capabilities identified earlier, placing special emphasis on

- Government-developed attack-response criteria, damage-reporting criteria, and recovery-priority criteria
- An IDR command, control, and reporting messaging system, including protocol and message format standard, to enable inter- and intra- IDR system communications
- One or more standards specifying content and format for entries in logs, history files, and so forth to facilitate exchange of information among IDR systems

This Page Intentionally Left Blank

List of References

1. LaPadula, L. J., September 1998, *CyberStrike Roadmap: Part 2 - Intrusion Detection and Reaction Architecture and Capabilities*, MTR 98B0000060, The MITRE Corporation, Bedford, Massachusetts.

2. LaPadula, L. J., September 1998, *The Air Force Tactical Environment: Characterizing the Data Networks for Information Protection Professionals*, MTR 98B0000044, The MITRE Corporation, Bedford, Massachusetts.

3. Godin, S. M., October 7, 1998, private communication, The MITRE Corporation.

4. National Security Telecommunications Advisory Committee, December 1997, *Report on the NS/EP Implications of Intrusion Detection Technology Research and Development*, Network Group Intrusion Detection Subgroup Report, President's National Security Telecommunications Advisory Committee.

5. Sandia National Laboratory, October 1996, *National Info-Sec Technical Baseline: Intrusion Detection and Response*, at URL: http://all.net/journal/ntb/ids.html on August 28, 1998, Lawrence Livermore National Laboratory, Sandia National Laboratory.

6. Hill, W. H., and S. J. Aguirre, September 1997, *Intrusion Detection Fly-Off: Implications for the United States Navy*, MTR 97W0000096, The MITRE Corporation, McLean, Virginia.

7. LaPadula, L. J., September 1998, *Intrusion Detection Work at MITRE: Fiscal Year 98*, PowerPoint Presentation, The MITRE Corporation, Bedford, Massachusetts.

8. LaPadula, L. J. and L. S. Volante, August 27, 1998, *CyberStrike Exploration: Vulnerability and Tool Database*, MTR 98B0000049, The MITRE Corporation, Bedford, Massachusetts.

This Page Intentionally Left Blank

Appendix

Reactions, Files, and Definitions for Compendium of Reactions

Reactions

Add to Monitor List: Add identification information of the attacker to the current Monitor list; send a Monitor report to the next higher command echelon.

Adjust Detection to Reduce False Alarming: A Sensor unit might modify a signature it is using to detect suspicious packets. A Director unit might send a command to a Sensor to disable certain signatures during specified times.

Alert: Notify another automated element of the IDR system or IDR personnel about an attack, a correlated possible attack, a discovered vulnerability, a hitherto unresolved intrusion discovered investigatively by review of logs.

Apply a Remedy for a Vulnerability: If possible, remove the vulnerability in the attacked system that allowed an intrusion to succeed by applying a known remedy. This may involve either automated capabilities or manual procedures or both.

Assess Damage: Based on an understanding of the attack that took place, determine the effects the damage had on the system or on the environment in which the system operates. An attack might disable certain functionality of the system or it might disable certain aspects of a mission because of potentially compromised information.

Carry Out Recovery Action: Take the necessary steps to restore the attacked system to as close to full operational readiness as possible. Some recovery steps may need to be carried out by personnel. This highlights the importance of determining recovery priorities for attacked systems.

Collect Forensic Data: Collect evidential data establishing the method used for an attack, the time of the attack, the damage caused by the attack, the source of the attack, the identity of the attacker, and so forth.

Correlate Possible Attacks: Analyze a set of possible attacks to discover whether they are related to each other in some way, such as by apparent source of attack. A set of possible attacks having highly correlated members may be evidence of an actual attack.

Determine Recovery Priority: Assign a priority to recovery efforts for repairing the damage caused by the attack. This action can be taken for a system that has been disconnected from execution of the mission as well as for a system that has continued to operate after an attack. Restoring a router to operation in the network might take priority over restoring an individual's workstation because loss of the router impairs mission

execution more than loss of the workstation. If automated, determining recovery priority would be done by a Director unit. To do so, it would need guidelines, which we might call recovery-priority criteria. These criteria might be augmented with input from IDR personnel.

Determine What the Vulnerability Is: Analyze the attack incident in light of the assumed probable or known site of a vulnerability to determine what the vulnerability is. This analysis may not succeed at all, or it may find only one of several vulnerabilities that contributed to the attack incident.

Determine Whether An Investigatively Discovered Intrusion Has Already Been Resolved: The IDR system searches files of resolved intrusions (History of Incidents files) to determine whether the intrusion it has discovered by investigation of audit and other logs has already been resolved. This capability requires extensive storage capacity and rapid retrieval ability; the more so as the investigative activity occurs at higher levels encompassing larger spans of interest.

Determine Whether Operation Can Continue: Assess the situation to quickly decide whether the system can continue to operate. This decision is based on whether it is likely that continued operation would impair mission execution. If, for example, a router's routing tables have been modified by an attack, its continued operation could seriously impair mission execution because there is the potential for it to send packets to wrong destinations. Subsequent analysis may reveal that damage to the routing tables was limited and can easily be repaired. For the time being, however, the router should be taken off line until damage assessment can be carried out. This assessment could result in a decision to change to a degraded mode of operation.

Determine Whether the Remedy Can Be Applied To The System: The IDR system determines whether the remedy can be applied to the system immediately. In some cases, doing so might not be desirable because it would disrupt operations. During execution of an important mission, it might be better to let a router continue functioning than to take it off line to rebuild its routing tables.

Determine Whether to Report Damage: Damage assessment may reveal minor damage about which a report to the IDR Director unit or to a higher echelon of command would serve little purpose. Major damage would be grounds for reporting if it adversely impacts mission execution whether directly or indirectly. To facilitate automated decision making in this area, guidelines, which we might call damage-reporting criteria, should be preestablished.

Determine Which System Has a Vulnerability: Analyze the attack incident or examine systems to determine which system within the protection domain has a vulnerability that might have allowed the attack to take place. This analysis may not be able to produce a definitive determination. It may only indicate a probable site of a vulnerability. This

action depends on the reaction system being able to either perform vulnerability scans itself or launch vulnerability scanning tools and use their reports.

Discover Whether the IDR System Has A Remedy For The Vulnerability: The IDR system queries its database of known vulnerabilities to discover whether it has a remedy for the vulnerability.

Log Intrusion in History File: Put information about the intrusion into the History file.

Log Possible Attack: Put information about the possible attack into the Possible Incidents log.

Make Adjustments to Automated Elements within Protection Domain: Make adjustments in policy, rules, configurations, or modes of operation of automated elements within protection domain. This might involve changing the policy of a firewall, changing the filtering rules of a router, changing the mode of operation of a server to a degraded mode or a special crisis mode.

Manipulate Connection: Take actions affecting the communication between the attacker and the monitor that will elicit additional useful information about the attacker, the attack methods, the location of the attacker, and so forth.

Monitor Attack: Allow the attack to proceed while controlling it and collecting information about it.

Monitor the Anomalous Circumstances: Periodically check whether the anomalous circumstances still exist, have diminished, or have worsened. The purpose is to resolve the situation, either erasing the possible attack or upgrading the possible attack to a verified attack.

Perform Triage: Do the quickest analysis possible to simply classify the attack as internal fault, verified attack, possible attack, or false alarm.

Report a Correlated Possible Attack: If the correlation analysis has been done by a Sensor or an Agent, the report is sent to the authorized Director within the IDR system. If the correlation analysis has been done by a Director, the Director sends an alert to lower level Directors or to its own Sensors and/or Agents.

Report Intrusion to Offensive IW Unit: Reports might be sent at the request of an offensive IW unit or as a request for counteraction in case the attack is persistent and cannot be thwarted by the defensive unit. One might typically expect such reports to be going to higher-authority echelons. It is conceivable that a request for action could reach a very high level involving international diplomatic activity.

Shut Attack: Take the necessary action to stop the attack of an intruder, such as terminating a TCP connection or changing a packet filtering policy.

Files

Name of File	Description of File
History of Incidents	A file of known incidents to be used for analysis and investigation (e.g., histograms, trends)
Possible Attacks	A file of information about current possible attacks (anomalies classified as possible attacks by triage). This file can be used for correlation analysis (see Reaction "Correlate Possible Attacks")
False Alarms	A file of information about false alarms. This file can be analyzed to determine performance of elements of an IDR system (for example, the Sensors) and possibly to reduce false alarming.

Definitions

Attack-Response Criteria: Guidelines for deciding whether to shut an attack or monitor it; the guidelines are based on factors such as criticality of the system, nature of the attack, and potential effect of the attack on the system.

Damage-Reporting Criteria: Guidelines for deciding whether to report damage caused by an attack; the guidelines are based on considerations of potential impact to mission execution. The reason for reporting the damage is to enable decision support systems to adjust allocation of resources, invoke contingency plans, and so forth.

False Alarm: A suspected attack that has been classified as a false alarm during the process of triage. A suspicious circumstance is classified as a false alarm when it is fully understood as a legitimate circumstance.

Internal Fault: An anomaly attributable to the operation or configuration of the system and not caused by actions of an intruder, user, or administrator.

Operationally Critical: The operationally critical system is one that is essential to execution of a current mission.

Possible Attack: Triage classifies an anomaly as a possible attack when it cannot explain the anomaly as an internal fault but also has not seen sufficient evidence to classify it as a verified attack.

Recovery-Priority Criteria: Guidelines for assigning a priority to recovery operations for a particular system. The guidelines are based on considerations such as when the system will be needed in its operational state and whether the time and personnel needed to perform the recovery are available.

Verified Attack: A suspected attack that has been classified as verified during the process of triage. Once classified as verified, the attack is treated as a real attack, even if there is not 100 percent assurance that the attack is real.