State of the Practice of Intrusion Detection Technologies

Julia Allen
Alan Christie
William Fithen
John McHugh
Jed Pickel
Ed Stoner

Contributors:
James Ellis
Eric Hayes
Jerome Marella
Bradford Willke

January 2000
Networked Systems Survivability Program

TECHNICAL REPORT
CMU/SEI-99-TR-028
ESC-99-028

Carnegie Mellon
Software Engineering Institute
Pittsburgh, PA 15213-3890

State of the Practice of Intrusion Detection Technologies

CMU/SEI-99-TR-028

ESC-99-028

Authors:
Julia Allen
Alan Christie
William Fithen
John McHugh
Jed Pickel
Ed Stoner

Contributors:
James Ellis
Eric Hayes
Jerome Marella
Bradford Willke

January 2000

Networked Systems Survivability Program

This work is sponsored by the Air Force Research Laboratory and the Air Force Computer Resources Support Improvement Program. The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense.

Please see http://www.sei.cmu.edu/publications/pubweb.html for information about how to order paper copies of SEI reports.

NO WARRANTY

THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

Use of any trademarks in this report is not intended in any way to infringe on the rights of the trademark holder.

Acknowledgments

This report was sponsored by the Air Force Research Laboratory (Mr. Dwayne Allain) and by the Air Force Computer Resources Support Improvement Program (Lt Col Joseph Jarzombek).

The authors acknowledge contributions made to this report, which were in the form of document production, interviews, and reviews of draft sections. The quality of the document was greatly enhanced by the expertise of the following individuals:

Ed Amoroso, AT&T
Jay Larrew, AFIWC (Air Force Information Warfare Center)
Teresa Lunt, Xerox
Roy Maxion, Carnegie Mellon University
Mark Woods, Internet Security Systems

Lincoln Laboratory:
Richard Lippman
Marc Zissman

MITRE:
Joshua Guttman
Leonard LaPadula
Marion Michaud
Jeffrey Picciotto

Software Engineering Institute:
Bunny Bernfeld
Claire Dixon
Mary Jonson
Tom Longstaff
Klaus-Peter Kossakowski
Jim Main
Mindi McDowell
Jacqueline Prause
Sheila Rosenthal
Tim Shimeall
Pam Williams

Table of Contents

State of the Practice of Intrusion Detection Technologies

List of Figures

List of Tables

Executive Summary

Attacks on the nation's computer infrastructures are a serious problem. Over the past 12 years, the growing number of computer security incidents on the Internet has reflected the growth of the Internet itself. Because most deployed computer systems are vulnerable to attack, intrusion detection (ID) is a rapidly developing field. Intrusion detection is an important technology business sector as well as an active area of research.

Vendors make many claims for their products in the commercial marketplace so separating hype from reality can be a major challenge. A goal of this report is to provide an unbiased assessment of publicly available ID technology. We hope this will help those who purchase and use ID technology to gain a realistic understanding of its capabilities and limitations. The report raises issues that we believe are important for ID system (IDS) developers to address as they formulate product strategies. The report also points out relevant issues for the research community as they formulate research directions and allocate funds.

Implementing intrusion detection systems on networks and hosts requires a broad understanding of computer security. The complexity of information technology infrastructures is increasing beyond any one person's ability to understand them, let alone administer them in a way that is operationally secure. Vendors are rapidly releasing new ID systems and aggressively competing for market share in an expanding market. Many products started out as point solutions. However, in response to consumers' inability to fully understand and use many ID systems, vendors are attempting to integrate approaches to solve a broader range of computer security problems. Evaluating ID systems is non-trivial and there is a lack of credible, comprehensive product evaluation information. Hiring and retaining personnel to competently administer security in general and intrusion detection in particular are increasing challenges. All of this rapid change makes it very difficult for an organization to implement an effective, long-term security strategy.

After reviewing the surveys cited in this report, one could conclude that ID technologies are becoming an accepted part of many organizations' information security tool suite. We are concerned that organizations are counting on these tools to solve a class of problems before they fully understand them. As a result, the solutions are likely to be inadequate or incorrect. Over-reliance on ID technologies can create a false sense of confidence about the degree to which tools are detecting intrusions against an organization's critical assets.

Both through our own experience and in discussion with technology experts and market analysts, we have observed that the current market condition of commercial ID tools and technologies exhibits a growing “bandwagon” effect. Each organization is comparing what they are doing with others in their peer group or market segment. If an organization views itself as taking security protection actions (such as deploying an IDS) that are equal to or slightly better than an organization that it considers its peer, that is good enough. At the decision-making level, there appears to be little or no regard for what ID systems can actually do. Nor is there an appreciation for the tasks that ID systems should not (or cannot) be relied upon to perform. Management’s priority appears to be to ensure that they can demonstrate that they have exercised a standard of due care in the event of any legal action. We believe that the vendor community is marketing to this condition through the product claims they make.

It remains to be seen whether or not intrusion detection technology can live up to the promise of accurately identifying attacks. The current generation of commercial ID systems uses a limited set of techniques to detect attacks. Attackers are rapidly improving their abilities to penetrate networks successfully — for example by developing ways to defeat ID systems themselves. Challenges to today’s ID systems include

- increases in the types of intruder goals, intruder abilities, tool sophistication, and diversity, as well as the use of more complex, subtle, and new attack scenarios
- the use of encrypted messages to transport malicious information
- the need to interoperate and correlate data across infrastructure environments with diverse technologies and policies
- ever increasing network traffic
- the lack of widely accepted ID terminology and conceptual structures
- volatility in the ID marketplace which makes the purchase and maintenance of ID systems difficult
- risks inherent in taking inappropriate automated response actions
- attacks on the ID systems themselves
- unacceptably high levels of false positives and false negatives, making it difficult to determine true positives
- the lack of objective ID system evaluation and test information
- the fact that most computing infrastructures are not designed to operate securely
- limited network traffic visibility resulting from switched local area networks. Faster networks preclude effective real-time analysis of all traffic on large pipes.

ID systems can provide useful, reliable results in specific situations and configurations. These include monitoring an organization's firewall policy to ensure it is implemented correctly, monitoring unpatched machines for specific vulnerabilities, and monitoring specific network services.

The key deployment consideration is to focus the IDS sensing and analysis activities on the most critical subnets and hosts so that a trained analyst can interpret and act on the data these activities produce to safeguard the most important assets.

This report presents recommendations for ID sponsors, users, vendors, and researchers. For sponsors, we recommend

- supporting ongoing, comprehensive testing of commercial ID systems and making test results publicly available
- emphasizing research funding directed towards reducing false alarms

For users, we suggest

- implementing a security architecture that reflects a defense-in-depth or layered approach to protecting an organization's assets, whether or not the organization chooses to deploy an IDS
- developing clear, concise IDS requirements based on security policy and organizational needs
- configuring the IDS to maximize performance. This includes selective deployment to monitor critical assets as well as signature tuning to prevent excessive false alarms.

We recommend that vendors

- support initiatives to create open source signatures
- move towards the distribution model used by the anti-virus community
- spend more time and resources testing signatures and making results public
- provide measures that represent the level of confidence a user should place in an ID system's ability to report an intrusion by type of signature or attack
- integrate human analysis as part of event diagnosis
- integrate available data sources more effectively to include information from different sensors and from different ID systems
- expand options for capturing forensic evidence

- increase efforts to detect malicious code (email attachments, Java, ActiveX)
- increase interaction with the research community

We believe that the research community can benefit the ID field by

- emphasizing the integration of diverse sources of available data to reduce false alarms
- providing credible, defensible test data to support test and evaluation of ID systems
- providing a taxonomy of vulnerabilities, i.e., a taxonomy that takes a victim rather than an intruder perspective
- developing approaches for defending against sophisticated attacks such as denial of service, insertion, evasion, and distributed, coordinated attacks
- developing approaches that integrate human analysis as part of event diagnosis
- developing approaches that support better detection of malicious code
- increasing interaction with the vendor community

This report does not emphasize current Department of Defense (DoD), Air Force (AF), and Defense Information Assurance Program initiatives in intrusion detection systems and technologies. Many of these efforts are specific to the DoD and involve proprietary products, systems, and documentation. In addition, we believe that the DoD and AF are well informed on the ID-related initiatives they are sponsoring. They are supported by other federally funded research and development centers (FFRDCs) (such as MITRE) in this area. Thanks to the Air Force Information Warfare Center (AFIWC), we have included a brief description of Government Off-the-Shelf (GOTS) ID efforts in Section 2.1.4. Our general approach was to analyze publicly available sources that could be of potential use to the DoD and to the general consumer, vendor, and research communities.

Preface

Because most deployed computer systems are vulnerable to an ever increasing threat of attack, intrusion detection (ID) is a rapidly developing field. Intrusion detection is an important technology business sector as well as an active area of research. Vendors make many claims for their products in the commercial marketplace so separating hype from reality can be a major challenge.

A goal of this report is to provide an unbiased assessment of publicly available ID technology. We hope this will help those who purchase and use ID technology to gain a realistic understanding of its capabilities and limitations. The report raises issues that we believe are important for ID system developers to address as they formulate product strategies. The report also points out relevant issues for the research community as they formulate research directions and allocate funds.

This report does not emphasize current Department of Defense (DoD), Air Force (AF), and Defense Information Assurance Program initiatives in intrusion detection systems and technologies. Many of these efforts are specific to the DoD and involve proprietary products, systems, and documentation. In addition, we believe that the DoD and AF are well informed on the ID-related initiatives they are sponsoring. They are supported by other federally funded research and development centers (FFRDCs) (such as MITRE) in this area. Thanks to the Air Force Information Warfare Center (AFIWC), we have included a brief description of Government Off-the-Shelf (GOTS) ID efforts in Section 2.1.4. Our general approach was to analyze publicly available sources that could be of potential use to the DoD and to the general consumer, vendor, and research communities.

Section 1 of the report provides an overview of ID technology from the perspective of the CERT® Coordination Center (CERT/CC).[1] The rapid growth in intrusion activity is fueling an increasing need for ID technology. This section provides context by citing examples that demonstrate how vulnerable networks and systems have become. It is followed by a review of the elements of attacks from the perspective of the attacker and of the victim. To convey how challenging it is to detect intruders, the dimensions of ID technology are characterized. Finally, this section reviews some of the challenges that confront the field of intrusion detection.

[1] CERT and CERT Coordination Center are registered in the U.S. Patent and Trademark Office. In response to the attack of the Morris worm in 1988, the Defense Advanced Research Projects Agency (DARPA) decided to create the CERT® Coordination Center (CERT/CC) at the Software Engineering Institute (SEI). The SEI was charged with establishing a capability to quickly and effectively coordinate communication among experts during security emergencies in order to prevent future incidents and building awareness of security issues across the Internet community. Since its inception in 1988, the CERT/CC has responded to more than 20,000 security incidents that have affected over 400,000 sites in the Department of Defense (DoD), other federal agencies, and the private sector. For more information, refer to the CERT/CC Web site at http://www.cert.org.

Section 2 provides an in-depth look at the current state of ID technology. The section starts with a review of research, commercial, and publicly available tools, and then examines the rate at which industry is adopting commercial products.

We describe some informal experiments we performed with a variety of commercial and research ID tools. Finally, we present what we believe are the some benefits and shortcomings of the current generation of ID tools.

Section 3 reviews a wide range of issues that need to be confronted if ID systems are to become an effective technology and suggests some solutions. Much of the vendor literature conveys a perception that if one installs an IDS, one no longer has to worry about undetected intrusions. Unfortunately, this is not the case. The issues are broad-ranging and include external pressures from attackers, human factors, and limitations in the current technology. While technology may solve part of the intrusion detection problem, it is likely to be ineffective unless it fits within the organization's business objectives and operations.

Section 4 suggests practices that an organization should adopt if they want to derive the greatest benefit from an IDS.

Section 5 provides recommendations for the intrusion detection sponsor, user, vendor, and research communities.

The appendices provide supporting information in several areas.

Appendix A defines terms as they are used in this report. Terminology is not applied consistently given the immaturity of the ID field so having a set of definitions is important.

Appendix B provides a list of references.

Appendix C defines acronyms used in this report.

Appendix D contains a review of selected ID technology literature, providing supporting detail for Section 2.1.

Appendix E identifies organizations and standards relevant to intrusion detection.

Appendix F provides a candidate set of criteria that can be used in selecting an intrusion detection system.

All sources (Appendix D) and related efforts (Appendix E) reviewed in preparation of this report are current as of January, 2000.

It is important to note that the scope of this report is also defined by what it does *not* address:

- a detailed technical explanation of intrusion detection principles and how the technology works
- operational issues associated with installing, deploying, and managing an IDS, other than as briefly described in Section 4
- threat management, including
  - the incorporation of IDS management within CSIRTs (computer security incident response teams)
  - the role of IDS in threat management, such as defining alarm severity, monitoring, alerting, and policy-based actions
  - the role of the IDS administrator (such as converting IDS logs into forensic evidence)
  - the development of event response procedures
  - the recommendation of enterprise-wide policies based on threats
- physical security including physical intrusion detection and intrusion detection systems

This report contains many Web references. The intrusion detection field changes rapidly and much information is posted first (and often only) on the Web. Many of these references either become out of date, are modified, or disappear altogether from the original site. During the development of this report, this was a problem. Consequently, we have downloaded a majority of the references into an electronic repository that we can access in the event Web pages are subsequently modified or removed from their original location. This is a somewhat unusual approach but, given the increasing dominance of the Web, we believe that it will become more prevalent.

As a cautionary note, we strongly urge you not to rely on Web references cited in this report (or any other report that is more than three months old) for detailed IDS product information unless you verify that the data is correct. This caution is extended to reports on details about attacks and how these attacks manifest themselves through various monitoring mechanisms.

1 Intrusion Detection — What Is It and Why Is It Needed?

1.1 The Seriousness of Cyber Attacks

Attacks on the nation's computer infrastructures are becoming an increasingly serious problem. Even though the problem is ubiquitous, government agencies are particularly appealing targets and they tend to be more willing to reveal such events than commercial organizations. This is demonstrated by the cases cited below. While statistics on the growth of attacks provide a more solid basis for justifying the need for intrusion detection (ID), case histories can often be more persuasive.

October 7, 1999: *Hackers apparently working from Russia have systematically broken into Defense Department computers for more than a year and took vast amounts of unclassified but nonetheless sensitive information, U.S. officials said Wednesday. Besides penetrating the Pentagon's defenses, the hackers have raided unclassified computer networks at Energy Department nuclear weapons and research labs, at the National Aeronautics and Space Administration and at many university research facilities and defense contractors, officials said.* [N9]

October 7, 1999: *At NASA, the attacks are "massive, really very massive," and "very, very surreptitious," NASA Inspector General Roberta Gross said in an interview. "It's difficult to tell what the damage is," Gross said. "They weren't shutting down systems. They were taking file listings, looking to see what's in people's directories." Gross said the intruders also installed "parking tools that they can use to get back in later." Such electronic "trap doors" may be used to evade detection devices and to secretly regain access.* [N9]

June 1, 1999: *After NATO jets hit the Chinese Embassy in Belgrade in May, hackers from China attacked a handful of U.S. government sites, including one maintained by the Energy Department. In an unrelated incident, the official White House site was shut down briefly because of an attempt to tamper with it by unidentified hackers, officials said.* [N1]

May 21, 1999: *"We successfully penetrated several mission-critical systems, including one responsible for calculating detailed positioning data for Earth-orbiting spacecraft and another that processes and distributes the scientific data received from these spacecraft," the General Accounting Office (GAO) said...Having gained access to these systems, the report* *said, "We could have disrupted NASA's ongoing command and control operations and stolen, modified, or destroyed system software and data."* [N3]

May 11, 1999: *The White House Web site was shut down today to determine whether hackers who tried to tamper with the site managed to do so. White House spokesman Barry Toiv said the site was shut down for 24 hours beginning late yesterday...MSNBC reported that there have been a series of politically motivated raids on government sites, undertaken in protest of last week's NATO bombing of the Chinese embassy in Belgrade, Yugoslavia. Unnamed government sources said the departments of Energy, Interior, and Labor as well as the U.S. Information Agency recently have been hit.* [N4]

April 6, 1999: *The nation's three nuclear weapons labs have shut down their classified computer systems for at least a week to beef up network security. Three preeminent Energy Department facilities halted operations Friday on all computers that handle secret information, in response to an unfavorable information security rating in a DOE audit of last year, according to Los Alamos National Laboratory spokesman Jim Danneskiold. The other two labs affected by the shutdown are Lawrence Livermore National Laboratory and Sandia National Laboratories...All three facilities will undertake several initiatives to improve security, including conducting computer security and threat awareness training; devising stricter access policies and tougher enforcement; implementing more rigorous procedures for transferring information from classified to unclassified computers; and establishing new intrusion detection measures.* [N5]

March 31, 1999: *NATO spokesman Jamie Shea said service on NATO's home page had been "erratic to say the least" since March 28, the fifth day of the alliance's bombing campaign against Yugoslavia. "It seems that we have been dealing with some hackers in Belgrade, who have hacked into our Web site," Shea told a news conference at NATO headquarters in Brussels. "At the same time, our email system has also been saturated by one individual who is currently sending us 2,000 emails a day. We are dealing with macro viruses from Yugoslavia in our email system," he said. A senior NATO diplomat said it was clear how well-organized and prepared Belgrade's offensive was: "It ranges all the way from organized ethnic cleansing to messing up our Web site."* [N6]

March 5, 1999: *The Pentagon today confirmed that attacks against U.S. military computers over the past few months are under special investigation by law enforcement and intelligence authorities. Deputy Defense secretary John Hamre briefed the House Armed Services Committee on the matter in a classified meeting February 23, according to the House Armed Services Committee. He warned legislators that the attackers were not merely individual hackers, and said part of the problem may stem from the cooperation of insiders within the U.S. military staff.... Hamre told the committee that the Pentagon detects between 80 and 100 hacker "events" every day. The Pentagon must investigate approximately one in ten of these.... One security expert said that while attacks from Russian and other foreign nations was* *nothing new, the new breed of hacks posed grave threats in their sophistication. "There is a steadily increasing number of these attacks," said Alan Paller, director of research for The SANS Institute. "And there are more of these that have three characteristics that set them apart." The first of these is that attacks are coming simultaneously from multiple, coordinated sites. The second is that the attacks are coming with more stealth, escaping the detection of intrusion monitoring systems by limiting the number of "pings," or connections. "These are coming in just under the detection threshold, at one every hour, or every three days," said Paller. "They're coming from patient people, who are usually more professional than children."* [N7]

September, 1998: *Hackers are banding together across the globe to mount low-visibility attacks in an effort to sneak under the radar of security specialists and intrusion detection software, a U.S. Navy network security team said today. Coordinated attacks from up to 15 different locations on several continents have been detected, and Navy experts believe that the attackers garner information by probing Navy Web sites and then share it among themselves. "These new patterns are really hard to decipher — you need expert forensics to get the smoking gun," said Stephen Northcutt, head of the Shadow intrusion detection team at the Naval Surface Warfare Center. "To know what's really happening will require law enforcement to get hold of the hackers' code so we can disassemble it."* [N8]

1.2 The Rapidly Growing Threat

The press releases in Section 1.1 reflect the serious and sophisticated nature of recent cyber-attacks. This is compounded by the fact that, over the past 12 years, the growth of incidents on the Internet has reflected the growth of the Internet itself. Figure 1-1 illustrates this growth by plotting the number of incidents reported to CERT/CC over those years. E-commerce can only exacerbate the upward trend in incidents. While in previous years, external attacks tended to originate from those interested in exploring the Internet for its own sake and testing their skills, there is an increasing trend towards intrusions motivated by financial, political, and military objectives. From a recent survey of 91 respondents [S33], there was an average loss of $256,044 per respondent's organization. While the survey indicated that internal breaches were still of greater concern, external attacks were increasing at an "alarming rate." The survey stated that "...the number of companies experiencing [penetration attacks] doubled from about 12 percent of all respondents in 1998 to 23 percent this year." Thus the stakes are being raised.

In the 1980s, intruders were the system experts (Figure 1-2). They had a high level of expertise and personally constructed methods for breaking into systems. Use of automated tools and exploit scripts was the exception rather than the rule. Today, absolutely anyone can attack a network — due to the widespread and easy availability of intrusion tools and exploit scripts that duplicate known methods of attack.

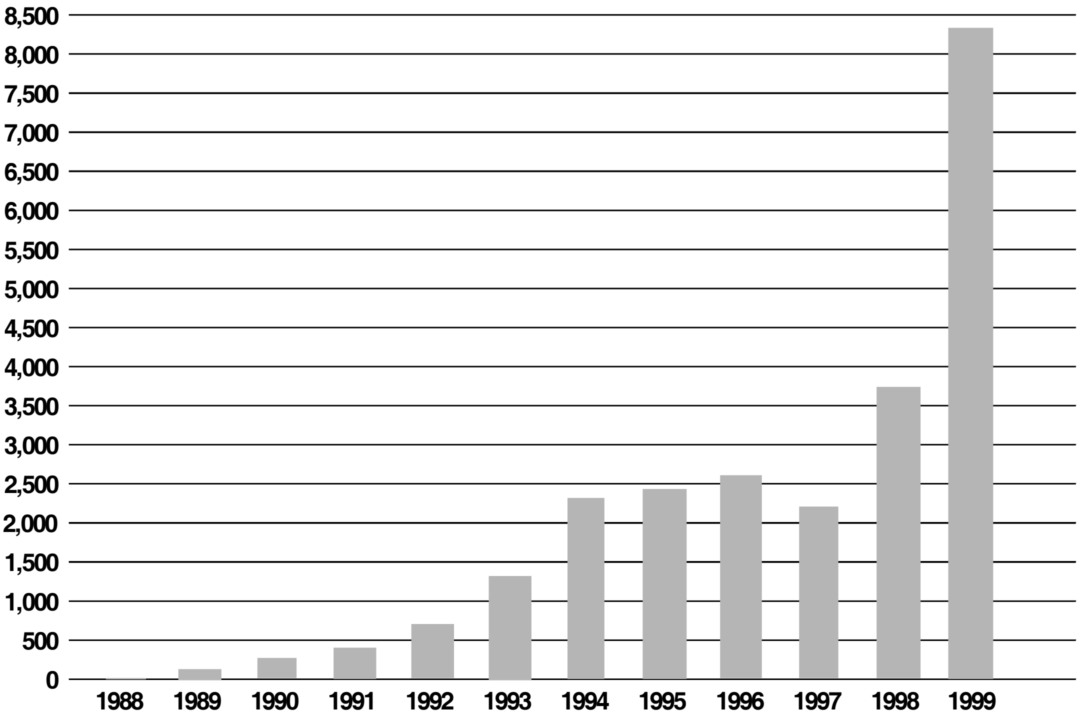

FIGURE 1-1: GROWTH IN NUMBER OF INCIDENTS HANDLED BY THE CERT/CC®

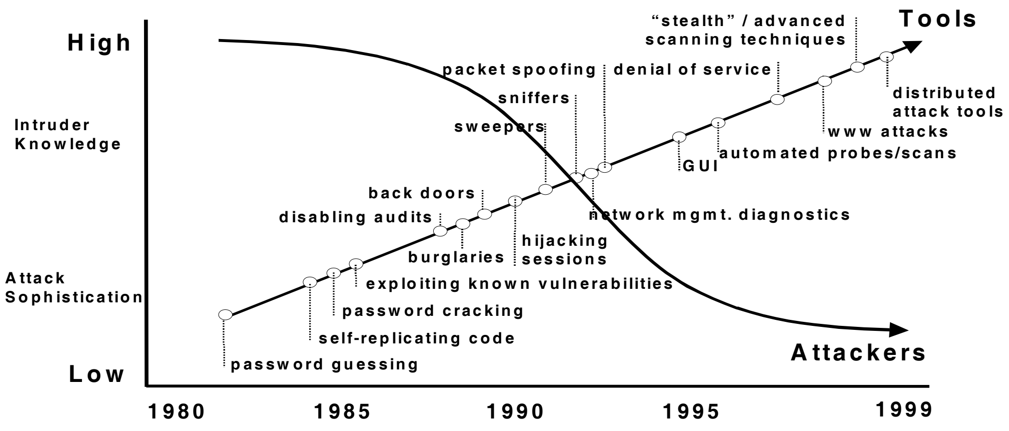

FIGURE 1-2: ATTACK SOPHISTICATION VS. INTRUDER TECHNICAL KNOWLEDGE

While experienced intruders are getting smarter, as demonstrated by the increased sophistication in the types of attacks, the knowledge required on the part of novice intruders to copy and launch known methods of attack is decreasing.

In the early/mid 1980s, intruders manually entering commands on their personal computer could access tens to hundreds of systems; today, intruders use automated tools to access thousands to tens of thousands of systems.[1] In the 1980s, it was relatively straightforward to determine if an intruder had broken into your systems and to determine their actions. Today, intrusions, and the damage they cause, can occur in a matter of seconds. Intruders are able to totally hide their presence by, for example, disabling commonly used services and reinstalling their own versions, and by erasing their tracks in audit and log files. In the 1980s and early 1990s, denial-of-service attacks were infrequent and not considered serious. Today, for organizations that conduct business electronically, such as online stock brokers and traders, a successful denial of service attack can put them out of business. As shown in Figure 1-1, from 1997 to 1998, we saw a 75 percent increase in the number of incidents reported to the CERT/CC. In 1999, the number of incidents increased by over 120 percent from 1998.

There are many reasons for the growing number and severity of attacks, including increased connectivity and complexity, increased availability of vulnerability information and attack scripts via the Internet, and dependence on distributed network services. As indicated by Donn Parker, the very nature of computer crime is that it is unpredictable, so you can’t use previous threats or attacks as a metric to prepare for future threats or attacks — the basis for all of today’s signature-based ID products [B91].

1.3 Attacker and Victim Perspectives on Intrusion

Attacks and intrusions can be viewed from a number of perspectives. The most common are those of the intruder and the victim. Each perspective brings with it distinct criteria for judging the success of the attack. Typically, we say that an intrusion has taken place when an attack is considered successful from the victim’s perspective, i.e., the victim has experienced some loss or consequence. A successful attack is enabled by the presence of a vulnerability in the victim’s system that is exploited by an intruder with an objective. We use the term intrusion to mean a successful attack.

An attack is unsuccessful from the perspective of the intruder if none of their objectives are fulfilled; whereas, a victim perceives an attack as unsuccessful if there are no consequences that result from the attack. Unsuccessful attacks from the perspective of an intruder may still have one or more consequences for a victim.

[1] Based on CERT/CC experience.

The intrusion process begins when an intruder takes steps to fulfill an objective. An essential component of an intrusion is taking advantage of one more vulnerabilities by using tools and exploit scripts.

The vulnerabilities exploited in this process can range from a flaw in a piece of software, such as a buffer overflow that can be exploited to elevate privileges, to a flaw in an organizational structure that allows a social engineering attack to obtain sensitive information or passwords to accounts. The intrusion process ends when some or all objectives of the intruder are realized or the intruder gives up.

Attacks can involve one or more attackers and one or more victims. Because multiple perspectives are involved in a single attack, defining what constitutes an attack is difficult. Is an attack an action taken by an adversary or is it the manifestation of that action as observed by the victim? Consider the example of the smurf attack [B92] where the attacker convinces a third party to perform an undesirable action against the intended victim. Is the attack the attacker pressing the enter key on the shell command to execute smurf? Is the attack the series of packets sent to the third party? Or is the series of packets observed at the victim site the attack? Or do all of these events fit together to define an attack?

Some example components of an attack from the perspective of an intruder are

- objective
- exploit scripts
- vulnerabilities in target system
- risk of carrying out an intrusion
- damage caused or consequences to victim

Components of an attack fall into either a known or an unknown category. Because attacks contain multiple components, it is possible that a single intrusion contains both. The concept of known and unknown varies from different perspectives of intrusion as well. An intruder does not necessarily know the consequences of an intrusion for a victim site or all of the hosts that were affected by an intrusion. Similarly, a victim does not necessarily know the objective of an intruder, the exploit scripts that are used, the vulnerabilities that are exploited, or the identity of the intruder.

Some example components of an attack from the perspective of a victim are

- What happened?
- Who is affected?
- How are they affected? (consequences)

- Who is the intruder?
- Where did the intrusion originate?
- When did the intrusion occur?
- How did the intrusion happen?
- Why did the intrusion happen?

The goal of intrusion detection is to positively identify all true attacks and negatively identify all non-attacks. The motivation for using intrusion detection technology may vary for different sites. Some may be interested in law enforcement including the tracking, tracing, and prosecution of intruders. Some may use intrusion detection as a mechanism for protecting computing resources, while others may be more interested in identifying and correcting vulnerabilities.

1.4 Dimensions of Intrusion Detection

Just as attacks can be viewed in different ways, so can the process of detecting them. Intrusion detection can result from the observation of an attack in progress or from recognizing the results of an intrusion after the fact. This section summarizes several characteristics of intrusion detection.

As the terms are used below, there is a discrepancy; the term intrusion is used to connote a successful attack and it is also used in the phrase “intrusion detection system” describing a system designed to detect attacks regardless of their success. To be semantically correct and consistent, we should use the phrase “attack detection system” to represent such a system; however, we continue to use the phrase “intrusion detection system” with the understanding that unsuccessful attacks are also represented.

1.4.1 Terminology

Intrusion detection is a young field, and many terms are not used consistently. As discussed above, there is even disagreement about what is meant by “intrusion” and “attack.” There are multiple terms used to represent various methods of detecting intrusions. This section clarifies the meaning of some important ID concepts as they are used throughout this report. A more complete set of definitions can be found in Appendix A.

- Analysis approaches
  An analysis approach is a method used by an IDS to determine whether or not an intrusion has occurred. There are two major categories of analysis approaches:
  - Attack signature detection (sometimes called “misuse detection”) identifies patterns corresponding to known attacks.

This includes passive protocol analysis which is the use of sniffers in promiscuous mode. It also includes signature analysis which is the interpretation of a series of packets (or a piece of data contained in those packets) that are determined, in advance, to represent a known pattern of attack [B26-b].

The attack signature may also be manifest in audit records, logs, or in changes in the compromised system.

  - Anomaly detection identifies any unacceptable deviation from expected behavior. Expected behavior is defined, in advance, by a manually developed profile or by an automatically developed profile. An automatically developed profile is created by software that collects and processes characteristics of system behavior over time and forms a statistically valid sample of such behavior. Note that unexpected behavior is not necessarily an attack; it may represent new, legitimate behavior that needs to be added to the category of expected behavior. A comparison between these approaches is given in Section 1.4.4.

- Attack
  An action conducted by one adversary, the intruder, against another adversary, the victim. The intruder carries out an attack with a specific objective in mind. From the perspective of an administrator responsible for maintaining a system, an attack is a set of one or more events that may have one or more security consequences. From the perspective of an intruder, an attack is a mechanism to fulfill an objective.

- Exploit
  The process of using a vulnerability to violate a security policy. A tool or defined method that could be used to violate a security policy is often referred to as an exploit script.

- False negative
  An event that the IDS fails to identify as an intrusion when one has in fact occurred [B26-b].

- False positive
  An event, incorrectly identified by the IDS as being an intrusion when none has occurred [B26-b].

- Incident
  A collection of data representing one or more related attacks. Attacks may be related by attacker, type of attack, objectives, sites, or timing.

- Intruder
  The person who carries out an attack. Attacker is a common synonym for intruder. The words attacker and intruder apply only after an attack has occurred. A potential intruder may be referred to as an adversary. Since the label of intruder is assigned by the victim of the intrusion and is therefore contingent on the victim's definition of encroachment, there can be no ubiquitous categorization of actions as being intrusive or not.

- Intrusion
  A common synonym for the word “attack”; more precisely, a successful attack. In this report, we often use the term intrusion to include attack, because the subject of the report is intrusion detection systems.

- Vulnerability
  A feature or a combination of features of a system that allows an adversary to place the system in a state that is contrary to the desires of the people responsible for the system and increases the probability or magnitude of undesirable behavior in or of the system.

1.4.2 ID System Components

The functionality of an IDS can be logically distributed into three components: sensors, analyzers, and a user interface.

- Sensors
  Sensors are responsible for collecting data. The input for a sensor may be any part of a system that could contain evidence of an intrusion. Example types of input to a sensor are network packets, log files, and system call traces. Sensors collect and forward this information to the analyzer.

- Analyzers
  Analyzers receive input from one or more sensors or from other analyzers. The analyzer is responsible for determining if an intrusion has occurred. The output of this component is an indication that an intrusion has occurred. The output may include evidence supporting the conclusion that an intrusion occurred. The analyzer may provide guidance about what actions to take as a result of the intrusion.

- User interface
  The user interface to an IDS enables a user to view output from the system or control the behavior of the system. In some systems, the user interface may equate to a “manager,” “director,” or “console” component.

In addition to these three essential components, an IDS may be supported by a “honeypot,” i.e., a system designed and configured to be visible to an intruder and to appear to have known vulnerabilities. A honeypot provides an environment and additional information that can be used to support intrusion analysis. The honeypot serves as a sensor for an IDS by waiting for intruders to attack the apparently vulnerable system. Having a honeypot serve as a sensor provides indications and warnings of an attack. Honeypots have the ability to detect intrusions in a controlled environment and preserve a known state.

1.4.3 Integrating Detection and Response

Intrusion detection and response have traditionally been thought of as two separate processes; however, the line between them is beginning to blur. As ID systems continue to evolve and improve, they are beginning to incorporate limited capabilities to respond to intrusions.

Typical responses to intrusions may include dropping suspicious traffic at the firewall, denying user access to resources as they exhibit anomalous behavior, or reporting the activity to other hosts or sites involved in the attack.

In Section 1.4.4, we describe a hierarchical model for intrusion detection systems, and explain that output from these systems tends to travel from the lower levels to the higher. Response data on the other hand may travel in either direction. For example, a network-based IDS may provide host-level response, such as modifying configuration files on particular hosts. Response may include updating configurations for other IDS components meaning that a response of one IDS or component could have an effect on the behavior of another IDS or component. For these reasons, detection and response systems are beginning to merge.

1.4.4 ID Systems “Hierarchy”

Although every IDS can be conceptually viewed as having a sensor, an analyzer, and a user interface, the types of data examined and the types of data generated by a particular IDS may vary significantly. ID systems can be classified into one of the following categories based on the types of data they examine:

- Application
  An application-based IDS examines the behavior of an application program, generally in the form of log files.

- Host
  A host-based IDS examines data such as log files, process accounting information, user behavior, or outputs from application-based ID systems operating on the host.

- Network
  A network IDS examines network traffic. It may have access to outputs from host-based and application-based ID systems operating within the monitored network environment.

- Multi-network/infrastructure
  A multi-network IDS generally takes the form of an incident response team (IRT), where the input of the system comes from “sites” within their constituency. A site in this case is an entity that lies within an administrative domain. Data communicated to this type of IDS is generally from application, host, network, or other multi-network intrusion detection systems.

The categories of ID systems listed above can be thought of as a hierarchy, the top of the hierarchy being multi-network or infrastructure-based ID systems and the bottom being application-based. An IDS at any point in the hierarchy could receive data from any level lower in the hierarchy in addition to a sensor that may operate at the same level. Output from an IDS can be utilized by other ID systems at the same or higher levels in the hierarchy.

1.4.5 A Comparison of ID Analysis Methods

There are distinct analysis methods for detecting known and unknown attacks. As discussed above, we defined these as attack signature detection and anomaly detection. In this section, we describe the differences between these two methods by examining several attributes.

- Knowledge
  Detecting intrusions requires either knowledge of possible intrusions or knowledge of the known and expected behavior of a system. In order for an IDS with a signature-based method to detect all attacks, it requires prior knowledge of all possible attacks. The IDS must recognize either the details of an attack or the patterns at a more abstract level that characterize the class of an attack. An anomaly-based system must have full knowledge of the expected behavior of the system to detect all attacks. In reality, neither of these is possible; they represent ideals.

- Ease of configuration
  Another attribute to consider is ease of configuration. A signature-based system in general requires significantly less configuration effort than a system to detect anomalies since the latter requires much data collection, analysis, and updating. Some systems allow users to create their own signature files which can increase the complexity of establishing the desired configuration.

  Anomaly-based systems in general are more difficult to configure because a comprehensive definition of known and expected behavior for a system is required. This demands that the user discover, understand, represent, and maintain the expected behavior of their system. In many cases, automated support is provided but this takes time to develop and the data that is used must be unambiguous.

- Reported data
  Signature-based ID systems generally produce conclusions based on pattern matching. The output of a signature-based system can vary from an alert message indicating that a particular signature has occurred to one that also provides supporting data that is relevant to the signature’s occurrence.

  The output of anomaly-based ID systems generally produce conclusions based on statistical correlations between actual and expected behaviors. Additionally, anomaly-based systems tend to produce more data since anything outside the realm of expected behavior is reported.

- Reporting accuracy
  Signatures that are not specific and anomaly profiles that are not adequately specified to describe expected behavior both result in ID systems that produce potentially large numbers of false positives and false negatives.

Depending on the environment within which an IDS is deployed, a combination of methods (signature and anomaly) for all types of ID systems (application, host, network, multi-network) may be required for the most effective solution. Signature-based ID systems are not able to detect all possible intrusions because of inherent detection limitations, constantly evolving attacks and exploits, new vulnerabilities, and use of new exploit scripts. Anomaly-based systems generally report a larger number of false positives as expected behavior changes.

An advantage of an anomaly-based IDS is the ability to detect novel attacks that can bypass signature-based systems. Such attacks can be analyzed by a person who can then define attack signatures. Using the combination of signature- and anomaly-based methods provides the capability to detect a larger variety of attacks and keep the signature-based system up to date.

1.5 Operational Challenges with Intrusion Detection Systems

Implementing intrusion detection systems on networks and hosts requires a broad understanding of computer security. The complexity of information technology infrastructures is increasing beyond any one person's ability to understand them, let alone administer them in a way that is operationally secure. Vendors are rapidly releasing new ID systems and aggressively competing for market share in an expanding market. Many products started out as point solutions. However, in response to consumers' inability to fully understand and use many ID systems, vendors are attempting to integrate approaches to solve a broader range of computer security problems. Evaluating ID systems is non-trivial and there is a lack of credible, comprehensive product evaluation information. Hiring and retaining personnel to competently administer security in general and intrusion detection in particular are increasing challenges. All of this rapid change makes it very difficult for an organization to implement an effective, long-term security strategy.

1.5.1 Growth in the Number and Claims of ID Products

Intrusion detection is an important and rapidly growing security technology market. International Data Corporation (IDC) reports revenues for these products increased 135 percent to $136 million in 1998 — and the growth is just getting started.

In 1999, the market was projected to grow almost 100 percent, and by 2003, it will approach $980 million [B93]. This market growth is driven by reports of steadily increasing number of computer security breaches; a 22 percent rise from 1996 to 1998, with $136 million in associated losses [B94]. Intrusion detection is considered by many to be the logical complement to network firewalls, extending the security management capabilities of system administrators to include security audit, monitoring, attack recognition, and response [B23].

Clearly, in this type of fast-paced, growing market, security product vendors are eager to capture market share and make claims that will support their efforts. However, regardless of vendor claims, ID systems do not have the capability to look at every possible security event. The event could have happened on a different network, the IDS itself could have been compromised, or the IDS might have reached its maximum bandwidth capacity and dropped further network traffic [B76]. Most commercial products have their own proprietary protocol for communications between the sensor detecting the event of interest and the analysis function that interprets the significance of the event — which makes it virtually impossible to correlate information from multiple ID systems or monitoring tools.

ID systems themselves are logical targets for attack [B26-b]. Smart intruders who realize that an IDS has been deployed on a network they are attacking will likely attack the IDS first, disabling it or forcing it to provide false information (distracting security personnel from the actual attack in progress, or framing someone else for the attack). In addition, many commercial and research ID tools have carried forward original design assumptions resulting in security weaknesses such as sending log files without encrypting them, absence of access control, and not performing integrity checks of ID system files.

1.5.2 Difficulty with Evaluating ID Technologies

It is extremely difficult to identify and evaluate the processes, procedures, tools, software, hardware, and databases that comprise the range of ID technologies. There is no industry standard against which to compare such systems because the technology is too new. The commercial ID new product cycle is very fast, based on the pace of the growing market. Northcutt [B76] recommends that you only use publications that are updated at least monthly as ID product buyer’s guides. Even after an organization has identified a list of candidate ID system solutions, the evaluation process will be quite complex if it is to provide the answers required to make an informed decision.

Marketing literature rarely describes how well a given IDS finds intruders and how much work is required to use and maintain that system in a fully functioning network with significant daily traffic. IDS vendors can specify which prototypical attacks can be found by their systems, but without access to the normal traffic generated by day-to-day work, they cannot describe how well their systems detect real attacks while passing background traffic and avoiding false alarms.

This information is critical: every declared intrusion requires time to review, regardless of whether it is a correct detection for which a real intrusion occurred, or whether it is merely a false alarm [B95].

Evaluating ID system capabilities requires test data; either network traffic (for network-based approaches) or profiles (of systems, processes, file use, and user behavior for host-based approaches). If you choose to do this yourself as part of the evaluation process, setting up the networks, operating environments, traffic samples (e.g., using live traffic or simulated “bad” traffic), and other supporting data is non-trivial and requires a significant investment of resources and time. Determining the intrusion detection approach employed by each product and the ways in which intrusions are detected is also non-trivial. These topics are described in more detail in Section 2.3 and 3.5.1.

Some organizations and standards groups are attempting to address many of the issues surrounding the selection and use of ID technologies. Several of these efforts are described in Appendix A.

1.5.3 Maintaining Necessary Knowledge

Given the constantly changing landscape of attacks and intrusions, you need to maintain several types of information (based on the IDS analysis approach) to ensure that your IDS continues to detect suspicious events. According to Amoroso [B89], this information includes

- profiles of normal and abnormal user, system, and process behavior
- strings that denote suspicious traffic patterns, including signatures of known attacks and intrusions
- information used to initiate response actions to various anomalies and attacks

Some of this information is likely maintained by the IDS vendor but not necessarily all. Staff responsible for the IDS should obtain the information in a secure manner and arrange for installed ID systems to be regularly updated (similar to operating system patches or new viruses being loaded into virus detection software). Any information not provided by the vendor must be maintained and applied when needed by technical staff.

1.5.4 Lack of Qualified Technical Staff

Technology alone is not enough to maintain network security. An organization needs qualified technical staff to evaluate, select, install, operate, and maintain ID technologies. In today’s market, there is a decreasing availability of the qualified intrusion analysts and system/network administrators who are knowledgeable about computer security.

According to Northcutt [B76], having an ID product do your “thinking/analysis” for you is a natural response to the lack of skilled technical people, particularly those with security skills. However, there are many attacks and probes occurring every day that are not canned “script kiddie” exploits. Only trained analysts with expert-class tools are going to be able to detect and analyze these.

As Amoroso indicates [B89], nearly all *reported* incidents in which an intruder has been caught in real time have involved manual intrusion detection methods used by attentive security experts. Furthermore, these incidents have involved locally developed ID tools and traps rather than commercial systems [B89]. Automation of the entire ID process is unlikely in the near future.

In the face of this reality, many organizations are choosing to outsource the ID operations, an option that comes with its own issues and risks (see Section 4.6 for further information).

1.5.5 Intrusion Detection as a Component of Defense-in-Depth

Intrusion detection is needed because firewalls cannot provide complete protection against intrusion. Experience teaches us never to rely on a single defensive line or technique. A firewall serves as an effective noise filter, stopping many attacks before they can enter an organization’s networks. However, firewalls are vulnerable to errors in configuration and ambiguous or undefined security policies. They are generally unable to protect against malicious mobile code, insider attacks, and unsecured modems. Firewalls rely on the existence of a central point through which traffic flows when the growing trend is towards geographically distributed networks with inside and outside users traversing the same subnets and, therefore, the absence of central points for firewall monitoring purposes. On internal networks, routers or switches can be configured to watch for signs of intrusion and take appropriate action based on what they detect [B76].

Implementing multiple layers of protection as part of an overall security architecture (such as firewalls, access control and authentication mechanisms, monitoring tools, vulnerability scanning tools, ID systems, security training) makes penetration by external intruders more difficult while making intrusion prevention and detection somewhat easier. See Section 4.5 for more details on this point.

2 What Is the Current State of Intrusion Detection Technologies?

This section covers a range of topics dealing with current ID technology and practice to illustrate where ID systems stand today. We start with a review of technology, looking at currently used tools in the research, commercial, and public domains. We then look at market conditions, summarizing several papers and surveys that describe the current market and where it is headed. We conclude by discussing some experiences with representative ID products that indicate why current ID systems are not the only solution to fix all security problems.

2.1 Survey of ID Technology

ID technology is immature and dynamic. Like the early auto manufacturers, new vendors appear, only to be absorbed by other vendors. The same is true with ID products (both commercial and research). Because of the rapid changes in the field, information such as lists, surveys, or reviews are quickly outdated. For example, a report by Staniford-Chen provides a summary of 42 ID-related products, but much has changed since its date of publication (winter 1997-1998).[1] Web-based lists (such as the one found in the SANS/NSA ID tools inventory) are easier to keep updated [B4].

As part of this effort, we conducted a wide-ranging review of ID literature. This review focuses mostly on materials accessible via the Web. Appendix B contains references to the articles reviewed in this section while Appendix D contains selected reviews.

Intrusion detection has been an active field of research for about two decades. This is exemplified by an influential paper, published in 1980, “Computer Security Threat Monitoring and Surveillance” by James Anderson [B34]. It was followed some years later (1987) by the seminal paper “An Intrusion Detection Model” by Dorothy Denning [S7]. Denning’s paper provides a methodological framework that inspired many researchers and, in more recent times, laid the groundwork for commercial products.

[1] In fact, the document and its URL were both revised while our report was being written. This change is reflected in the bibliography. A reference to the new document can be found in Appendix B [S12].

There are six main topic areas covered by the survey: ID surveys, taxonomies, testing and evaluation, research, commercial tools, and ID directions (all are further elaborated in Appendix D). The papers that are more relevant to this review are discussed more fully, while other papers are simply cited because they are useful resource materials. In all cases, the reviews are brief and are provided so that the reader can selectively target relevant papers. Each review follows the same structured table-based format.

This section presents some research and commercial products that are examples of available ID technology, as well as a few products available in the public domain.

2.1.1 Examples of Research Products

ID research performed in the early 1990s produced a number of new tools [S6]. However, many were developed by students to explore concepts, and after they moved on, the tools were not maintained. Nevertheless, these tools influenced the direction of subsequent research efforts and also of commercial ventures. Early efforts often focused on host-based solutions, but because of the explosive growth of networking, later efforts concentrated on network-based systems.

The tools reviewed here reflect a core of active research that has evolved from earlier efforts. The first two, EMERALD and NetSTAT, have matured a great deal and compliment each other's approaches. The third research tool discussed is Bro. It is unique in addressing the issue of network penetration through attempts to overload or confuse the ID system.

2.1.1.1 EMERALD

EMERALD (Event Monitoring Enabling Responses to Anomalous Live Disturbances) is the most recent research tool developed by SRI International. This line of tools has explored issues in intrusion detection associated with both deviations from normal user behavior (anomalies), and known intrusion patterns (signatures). SRI's pioneering work in intrusion detection began in 1983 when a multivariate statistical algorithm was developed to discriminate between different user behaviors [R1-d].

Somewhat later, the use of a signature analysis subsystem, based on the P-BEST [R33] expert system was investigated to support detection of suspicious activities. These research efforts were incorporated into SRI's early intrusion detection system, IDES [R1-b], a system that monitors activity on multiple hosts in real time.

Based on experiences with IDES, a re-achitected, production-oriented tool, NIDES [R1-c], was developed between 1992 and 1994. Like IDES, this tool is host-based, and uses the P-BEST production rule system.

However, it went further by adding a component called RESOLVER that fuses the results from the statistical and signature analysis components. The user interface in NIDES was also a significant improvement over the IDES user interface.

EMERALD builds on the earlier IDES/NIDES experiences but this time focuses on support for networks rather than for a collection of hosts. A major goal of EMERALD is to address issues associated with large, loosely coupled enterprise networks. Such environments are more difficult to monitor and analyze due to the distributed nature of the incoming information. EMERALD structures users into a federation of independently administered domains. Each domain provides a collection of network services, such as http or ftp, that may have different trust relationships with each other, and across which different security policies may apply. In this context, one centralized repository is likely to result in significant performance degradation, as is the centralized analysis of all the data. These issues motivated the work on EMERALD and the demonstration of “divide and conquer” techniques that it investigated.

The hierarchical approach provides three levels of analysis performed by a three-tiered system of monitors: service monitors, domain monitors, and enterprise monitors. These monitors have the same basic architecture: a set of profiler engines (for anomaly detection), signature engines (for signature analysis), and a resolver component that integrates the results generated from the engines.

Each module also contains a resource object that provides a configurable library of information to customize the module’s components to the target application.This object can be re-used in multiple monitors within an EMERALD application. At the lowest level, service monitors support intrusion detection for individual components and network services within one domain, probing for or reading data (activity logs, events, etc.), and performing local signature and statistical analyses.

Domain monitors integrate information from the service monitors to provide a domain-wide view of intrusions, while the enterprise monitors perform inter-domain analysis to assess threats from a global perspective. Of interest at the enterprise level are such threats as worm-like attacks and inter-domain attacks on network services. Subscription-based communication channels allow different service monitors to communicate with each other, either by having information directed from one monitor to another (“pushed”) or requested by one monitor from another (“pulled”).

Prior work with NIDES demonstrated that statistical profiling techniques could be effective with either users or applications as targets. The monitoring of applications (e.g., anonymous FTP), was particularly effective since fewer application profiles were required. EMERALD generalizes the profiling technique by abstracting the notion of a profile, separating profile management from profile analysis.

With respect to signature analysis, service-layer signature engines monitor domain components to determine if abnormal activity is occurring through known exploit scripts. Signature engines in higher-level monitors distill this information to assess if a broader attack is occurring. In addition to integrating the results from the statistical and signature engines, the resolver component provides other functions. These include providing a subscription service that allows a third party tool to be integrated into the EMERALD environment, acting on reports generated by the statistical and signature engines, providing an interface to the monitor administrator, and initiating attack countermeasures, such as terminating processes.

EMERALD is a work in progress. It provides an example of the direction that future intrusion detection systems may take. As intruders become more sophisticated in their attacks, they will be increasingly likely to disperse the evidence of their work across networks, making it difficult to sense when a distributed/coordinated attack is occurring. In such situations, the ability to collect, assimilate, correlate, and analyze information emanating from diverse sources in real time becomes essential. The flexibility of EMERALD's scalable architecture, its ability to abstract functionality, its openness to the addition of external tools, and the prior experience (e.g., with NIDES) that is reflected in its functional components, makes EMERALD a forerunner of future ID tools. However, managing and maintaining the information base and building the system's infrastructure may require significant effort.

2.1.1.2 NetStat

NetSTAT is the latest in a line of "STAT" research tools produced by the University of California at Santa Barbara. The STAT activity, started in the early 1990s, explores the use of state-transition analysis in support of real-time intrusion detection [R4]. The approach is based on the premise that certain sequences of actions reflect unauthorized activity and indicate an intruder moving the system from an initial authorized state to a compromised state.

Most host-based intrusion detection systems in the anomaly category analyze evidence for intrusion in the computer's audit trail. However, in the STAT approach, the audit trail information is transformed through an "audit trail analyzer" that filters and abstracts the information gathered at the audit trail level. These abstractions, which are more suitable for analysis, portability, and human understanding, are called signatures and are central to the STAT approach. Signature actions move the system through the sequence of states, each state driving the system closer to a compromised configuration. Intrusion sequences are defined by state transitions that are captured in production system rule-sets.

The initial implementation of the method was a host-based, UNIX-based system called USTAT [R4]. USTAT was composed of

- *a preprocessor*
- *a knowledgebase (that included a fact base and rule base)*

- *an inference engine*
- *a decision engine*

The preprocessor filters and manipulates the data into a form that is audit-file independent. The rule base component of the knowledgebase stores the state-transition rules that indicate the predefined intrusion sequences, while the fact base stores the dynamically changing state of the system with respect to possible ongoing intrusions.

Given new information generated by the preprocessor together with the current system state as defined in the fact base, the inference engine identifies any significant state changes and updates the fact base. An update function then revises the fact base to reflect these changes. The inference engine also notifies a decision engine of possible security violations. The decision engine in turn either notifies the site security officer of the event or initiates action on its own. One advantage of the state-driven approach is that an attack may be recognized and acted on prior to reaching the compromised state.

This state-based approach uses an inference engine table to track each possible intrusion, and allows USTAT to identify a coordinated attack emanating from multiple sources. It can do this since attack sequences are defined, not by who is perpetrating the attack but by states of the system. Thus, if two attackers are relying on the same composite state of the system, each of their subsequent actions can be followed through a fork in the previous state transition sequence. This forking is implemented by duplicating rows in the inference engine table, each row representing different attack sequences.

NSTAT [R3] was the natural successor to USTAT. NSTAT focused on supporting a network of hosts in which, for example, files are shared. Thus actions on one host, such as mounting directories, can influence other machines on the network. Having one centralized detection system results in less performance impact on the local hosts and also allows for more informed intrusion analysis when a multi-host attack is being perpetrated. With NSTAT, the local hosts convert audit data into NSTAT format and merge the data steams into one.

The most recent of the tools, NetSTAT [R30], is currently under development and diverges from the prior host-based systems by addressing network intrusion. NetSTAT is composed of a set of probes that are responsible for detecting and evaluating intrusions in the sub-networks to which the probes are attached. Each probe is supported by a remotely configurable data filter, an inference engine, and a decision engine. These probes can act autonomously. However, different parts of the network may detect components of an intrusion (because of the differing locations and filters). If an intrusion component is detected, then an event can be forwarded to other interested probes that subscribe to that event in order to get a more complete understanding of the intrusion. Thus, intrusions that involve separate subnetworks can be identified.

The probes are supported by an analyzer, a stand-alone tool that supports the generation and management of probes. The analyzer is composed of a network fact base, a database of state-based intrusion scenarios, an analysis engine, and a configuration builder.

It determines which events should be monitored for, where they should be monitored, what network topology information is required, and what network state information is required to support the intrusion analysis. To perform these actions, the analysis engine uses information in the network fact base together with the scenario database to define attacks to which the network may be vulnerable. This information is passed to the configuration builder that in turn generates the probe configurations. These probe files consist of a filter, state-transition information, and the decision tables that allow the probe to execute.

2.1.1.3 Bro

Bro is a research tool being developed by the Lawrence Livermore National Laboratory. It is being built, in part, to explore issues related to the robustness of intrusion detection systems, i.e., assessing what characteristics make an ID system capable of resisting attacks against itself. The design goals for Bro [R31] include

- *high-load monitoring. The ability to handle high data transfer rates and traffic volumes without dropping packets is important. An intruder could use the mechanism of overloading the network with extraneous packets to flood the ID system. This could force the ID system to drop packets to which the network was vulnerable.*
- *real-time notification. This is needed to assure timely response to intruder threats.*
- *decoupling mechanism from policy. Separating the data filtering, event identification and policy reactions to the events results in a cleaner software design, easier implementation, and more straightforward maintenance.*
- *system extensibility. The large number of known attacks, together with the aggressive uncovering of new vulnerabilities, requires that Bro have the ability to rapidly add new attack scripts to its library.*
- *an ability to ward off attacks. Sophisticated attackers will likely probe for weaknesses in intrusion detection systems themselves.*

Bro has a three-level hierarchy of functions. At the lowest level, Bro uses libpcap, a utility to extract packets from the network. This decouples the main intrusion detection functionality of Bro from the networking details. This also allows a significant fraction of the packets entering the network to be rejected at a low level. Thus libpcap will capture all packets associated with the application protocols (e.g., finger, ftp, telnet) of which Bro is aware.

The next layer, the event layer, performs integrity checks on packet headers. If the header is ill-formed, an event identifying the problem is generated, and the header is discarded. A check is then performed to determine if the full contents of the packet should be recorded (usually if