

Intrusion Detection: Systems and Models

Joseph S. Sherif

California Institute of Technology, JPL, Pasadena, CA 91109

California State University, Fullerton, CA 92834

Jsherif@fullerton.edu

Tommy G. Dearmond

California Institute of Technology, JPL, Pasadena, CA 91109

tdearmond@jpl.nasa.gov

Abstract

Organizations more often than not lack comprehensive security policies and are not adequately prepared to protect their systems against intrusions. This paper puts forward a review of state of the art and state of the applicability of intrusion detection systems, and models. The paper also presents a classification of literature pertaining to intrusion detection.

1. Introduction

Too frequently today there are headlines about the latest hacker attack. They have broken into another system. They have stolen credit card lists. They have stolen military secrets. They had stolen trade secrets.

Books like:

- The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage, Stoll [178].
- Takedown, The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw—By the Man Who Did It, Shimomura [164].
- The Hacker Crackdown, Sterling [176], and
- Masters of Deception: The Gang That Ruled Cyberspace, Slatalla [168].

certainly make for interesting reading. And they tell stories of extensive and sustained attacks against many computer systems. These were systems that in many circumstances were thought to be secure. And individuals who were determined and relentless in their pursuit carried out the attacks from “unsophisticated” computer installations—like garages and apartments—. Some did it just to prove it could be done, and because in some circles a successful attack was a

recognized achievement of the first rank. Others carried out their attacks to create mischief, and to cause the greatest amount of havoc and damage.

Though one might think that with some 40 years (if, for the sake of discussion we posit 1960 as the “beginning” of the age”) of modern computing as we know it, surely the attacks must be isolated incidents. Surely, the technologies to defend computer systems should be commonplace. But such is simply not the case. In fact, it can be shown that the incidence of computer intrusion is growing, perhaps at an alarming rate.

Mahoney [118] defines at least six types of computer attacks.

- Worms—self-replicating programs that spread across a network.
- Viruses—programs that replicate when a user performs some action such as running a program.
- Server attacks—a client exploits a bug in the server to cause it to perform some unintended action.
- Client attacks—a server exploits a bug in a client to cause it to perform some unintended action.
- Network attacks (denial of service)—a remote attacker exploits a bug in the network software or weakness in the protocol to cause a server, router, or network to fail.
- Root attacks—a user on a multi-user operating system obtains the privileges of another user (usually “root”) by either obtaining the other

user's password, or bypassing controls that restrict access.

2. Literature survey

2.1 Intrusion Detection Systems

Though the public awareness of the whole area of "intrusion detection" seems to have been more recent, it is certainly not a new area of inquiry. In fact, it has been an area of concern for most of what we know of "modern" computers. There have been a number of important milestones in the brief history of Intrusion Detection Systems. The following list is consolidated from multiple sources [1, 3, 19, 53, 77-80, 101,111,138, 141, 157, 161, and 179].

- **1960's:** The emergence of time-sharing systems demonstrated the need to control access to computer resources.
- **1970's:** The DOD Ware Report pointed out the need for computer security.
- **1970's (Mid to late):** A number of systems were designed and implemented using security kernel architectures.
- **1980:** Anderson [6] first proposed that audit trails should be used to Monitor threats. The importance of such data had not been comprehended at that time and all the available system security procedures were focused on denying access to sensitive data from an unauthorized source.
- **1983:** The Department of Defense Trusted Computer System Evaluation Criteria-- the "orange book"--was published and provided a set of criteria for evaluating computer security control effectiveness
- **1987:** Denning [31-33] presented an abstract model of an Intrusion Detection Expert System (IDES). Her paper was the first to propose the concept of intrusion detection as a solution to the problem of providing a sense of security in computer systems.
- **1988:** The Internet Worm program of 1988--which infected thousands of machines and disrupted normal activities for several days--was detected primarily through manual means.

Lunt [110-116] refined the intrusion detection model proposed by Denning and created the IDES prototype system. This system

was designed to detect intrusion attempts with adaptation to gradual changes in behavior to minimize false alarms.

Smaha [170] developed the Haystack system in order to assist Air Force Security Officers detect misuse of the mainframes used at Air Force Bases

Sebring [160] developed MIDAS (Multics Intrusion Detection and Alerting System) to monitor the National Computer Security Center Dockmaster system.

- **1989:** Wisdom and Sense from the Los Alamos National Laboratory, and Information Security Officer's Assistant (ISOA) from Planning Research Corporation, Vacaro [188].
- **1990:** A new concept was introduced in 1990, with NSM (Network Security Monitor, now called Network Intrusion Detector or NID): instead of examining the audit trails of a host computer system, suspicious behavior was detected by passively monitoring the network traffic in a LAN, Heberlein [63].
- **1991:** A different idea was introduced with NADIR (Network Anomaly Detection and Intrusion Reporter) and DIDS (Distributed Intrusion Detection System): the audit data from multiple hosts were collected and aggregated in order to detect coordinated attacks against a set of hosts, Jackson [76-79] and Hochberg [69].
- **1994:** Crosbie and Spafford [25,26] suggested the use of autonomous agents in order to improve the scalability, maintainability, efficiency and fault tolerance of an IDS. This idea fit well with the ongoing research on software agents in other areas of computer science.
- **1995:** An improved version of IDES was developed in 1995, called NIDES (Next-generation Intrusion Detection Expert System), Javitz [80].
- **1996:** The design and implementation of GrIDS addressed the scalability deficiencies in most contemporary intrusion detection systems. This system facilitates the detection of large-scale automated or coordinated attacks, which may even span multiple administrative domains, Cheung [22] and Staniford [174].

- **1998:** Anderson and Khattak [4] offered an innovative approach to intrusion detection, by incorporating informational retrieval techniques into intrusion detection tools.

Table 1 gives bibliographic references on intrusion detection under various classifications for ease of use by the reader.

Table 1 Classification of Intrusion Detection (ID) under Relevant Areas.

Intrusion Detection Relevant Area	References
1. ID Concepts, Theory and Methodology	Axelsson [9], Bace [10], Dias [34], Dowell [37], Dunigan [38], Enterasys [39], Escamilla [40], Eskin [42], Forte [48], Graham [53], Gross [54], Halme [58], Heody [59], Heberlein [60, 61, 62, 64], Helman [66], Hubbard [71], Ilgun [72, 75], Internet Eng. [76], Jackson [77], Kossakowski [83], Kumar [84], Lee [91,96,101], Liepins [104], Lunt [111, 112], Mahoney [118], Maiwald [119], Mansfield [121], Marceau [122], Mark [124], McAuliffe [125], McConnell [126], Mukherjee [134], Northcutt [137-138], Pichnarezyk [145], Puketza [152, 153], Reavis [154], Scambray [158], Sherif, Ayers, Dearmond [161], Snap [171], Sommer [173], Sundaram [179], Ting [184], Wood [200], Yip [202], Yuill [203], Zamboni [204], Zerkle [206], Kim [81], Blain [17], Debar [28], Puketza [152, 153]
2. Autonomous Agents, Expert Systems	
-General	Crosbie [26], Purdue University [8]
-AudES: Audit Expert Systems	Tsudik [187]
-AID System	Sobirey[172]
-Bro Real Time Intrusion Detection	Paxon [142, 143]
-CIDF: Common Intrusion Detection Framework	Staniford [175]
-COAST	Balasubramaniyan [12]
-Clustering	Portnoy [149]
-Data Mining	Lee [91, 93, 94-101]
-Discovery	Jener [180]
-EMERALD: Event Monitoring Enabling	Neumann [135], Porras [147]
-ESSENSE	Valcarce [189]
-GASSATA Genetic Algorithm	Cedex [2], Crosbie [25], Ladovic [128], Me [127]
-GrIDS: Graph Based Intrusion Detection System	Cheung [22], Staniford [174]
-Haystack	Smaha [170]
-Hobids: Host-based Intrusion Detection System	Hershkop [67], Lee [93, 94, 97-100, 102], Mandanaris [120]
-IDAMN: Intrusion Detection Architecture for Mobile Networks	Samfat [156], Didier [135]
-IDES: Intrusion Detection Expert System	Denning [31-33]
-MIDAS: Multics Intrusion Detection and Alerting System	Sebring [160]

-Machine Learning	Frank [49], Tener [180], Weiss [194], Lane [87, 88]
-Markov Chain	Ye [201]
-NIDX: Network Intrusion Detection	Bauer [13]
-NADIR: Network Audit Director and Intrusion Reporter	Hochberg [69]
-NIDES: Next Generation Intrusion Detection Expert System	Anderson [3], Lunt [113-116], Sebring [160]
-Neural Networks	Debar [27], Ghosh [52], Simonian [166]
-Nonparametric Pattern Recognition	Lankewics [90]
-NSM: Network Security Monitor	Heberlein [63]
-Petri Nets	Frincke [58]
-Phased Approach Expert System	Jackson [78, 79]
-Pattern-based, Peer-based, Rank-based	Garvey [51], Ilgun [74], Mounji [133], Porras [148], Shieh [163], Sinclair [167], White [196]
-RETISS: Real-Tie Security System Using Fuzzy Logic	Carrettoni '20]
-SAINT: Security Analysis Integration Tool	Zamboni [206]
-SNORT	Roesch [155]
-SNMS: Shadow Network Mgt. System	Ong [140]
-STAT: State Transition Analysis Tool	Porras [145]
-Statistical Approach	Marchette [123]
-Visual Model	Vert [190]
-Wisdom and Secure	Vacaro [188]
3. Audit, Analysis, Monitoring, Surveillance	Bishop [14-16], Cedex [21], Ko [82], Schaen [159], Sibert [105], Wee [192, 193], Wetmore [195], Amoroso [2], Anderson [6], Apap [7], DeDios [29], Brentano [18], Mell [129], Habra [55-56], Helman [65], Lunt [110], Moitra [132], Piccioto [144], Teng [182]
4. ID Evaluation	Lindquist [105], Lippman [106, 107], Lodin [108], Lundin [109], MIT [131], Northcutt [139], Anderson [4, 5], Allen [1], Carnegie Mellon [19], Bace [11]
5. Anomaly Detection	Eskin [41], Liepins [103], Seleznyov [161], Teng [183], Winkler [192-199], Mahony [117], Vaccaro [188], Lee [97-100]
-Misuse	Jackson [79], Kumar [85, 86], Neumann [136], Smaha [168, 169], Levitt [102], Price [150], Corbitt [24]
-System Calls	Eskin [44], Hofmeyer [70], Warrender [191]
-Adaptive	Eskin [43], Fan [45], Feiertag [47], Halme [57]
-Feature Selection	Doak [36]
-Network Based	Denmac [30]
-Host Based	Zirkle [207]
-Behavior Based	Herve [68], Ye [201]
-Cooperative	Cheung [23], SANS [157]
-Cost Sensitive	Fan [46], Lee [95], Miller [130], Panagiotis [141], Stolfo [177]
6. General References	Amoroso [2], Marchette [123], Proctor [151], Shimomura [164], Sterling [176], Stoll [178], Toxen [185], Bace [10], Escamilla [40], Northcutt [40], Toxen [186], Proctor [151], Schneier [159], Spitzner [173].

Intrusion is defined by Lodin [108] as “any set of actions that attempts to compromise the integrity, confidentiality or availability of a resource”. He also notes that an intrusion is “the act of a person or proxy attempting to break into or misuse one’s system in violation of an established policy.” Sundaram [179] noted that an intrusion threat is the potential possibility of a deliberate unauthorized attempt to access information, manipulate information, or render a system unreliable or unusable. With this perspective, Sundaram also noted that there are different aspects to an intrusion, each of which is significant to a full analysis and response. These aspects include [179]:

- Risk: Accidental or unpredictable exposure of information, or violation of operations integrity due to the malfunction of hardware or incomplete or incorrect software design.
- Vulnerability: A known or suspected flaw in the hardware or software or operation of a system that exposes the system to penetration or its information to accidental disclosure.
- Attack: A specific formulation or execution of a plan to carry out a threat.
- Penetration: A successful attack -- the ability to obtain unauthorized (undetected) access to files and programs or the control state of a computer system.

Intrusions can be classified into two major classifications. Lodin [108] categorized Intrusions into the following classes: (1) Misuse intrusions are well-defined attacks against known system vulnerabilities. They can be detected by watching for specific actions being performed on specific objects, and (2) Anomaly intrusions are

based on activities that are deviations from normal system usage patterns. They are detected by building a profile of the system or users being monitored, and detecting significant deviations from this profile.

One significant contribution to the subject of intrusion classification was made by Lindqvist [105] who noted that previous work directed at intrusion classification was less than adequate for the basis of research. Classifications that focused on the intruders and their methods (that is the threat or intrusion technique) tended to focus on the exploitation, but did so in terms of the technique used. Classifications that stressed the characteristics of the computer system that make the intrusion possible (that is the vulnerability or security flaw) frequently did not account for the exploitation of known flaws. Lindqvist [105] believes that proper intrusion classification is essential for the following reasons:

- In general, categorizing a phenomenon makes systematic studies possible.
- An established taxonomy would be useful when reporting incidents to incident response teams, such as the CERT Coordination Center.
- If the taxonomy included a grading of the severity impact of the intrusion, system owners and administrators would be helped in prioritizing their efforts.

Lindqvist [105] also cited the work of Neumann and Parker [136], which was, based on an analysis of 3, 000 computer-abuse cases over a 20-year period. The Neumann and Parker classification is summarized in the following tables.

Table 2. Computer Misuse Techniques [136]

Class	Description
NP1: External misuse	Generally non-technological and unobserved, physically separate from computer and communication facilities; for example, visual spying.
NP2: Hardware misuse	1. Passive, with no (immediate) side effects. 2. Active, with side effects.
NP3: Masquerading	Impersonation; playback and spoofing attacks; etc.
NP4: Setting up subsequent misuse	Planting and arming malicious software.
NP5: Bypassing intended controls	Circumvention of existing controls or improper acquisition of otherwise denied authority.
NP6: Active misuse of resources	Misuse of (apparently) conferred authority that alters the system or its data.
NP7: Passive misuse of resources	Misuse of (apparently) conferred reading authority.
NP8: Misuse resulting from inaction	Failure to avert a potential problem in a timely fashion, or an error of omission.
NP9: Use as an indirect aid in committing other misuse	1. As a tool in planning computer misuse; etc. 2. As a tool in planning criminal/unethical activity.

Another issue for Lindqvist was the question of intrusion consequences. He considered that both the immediate result of the breach, as well what the intruder did after the initial breach were both important. Lindqvist [105] taxonomy encompasses the following properties:

- The categories in a taxonomy should be mutually exclusive (every specimen should fit in at most one category) and collectively exhaustive (every specimen should fit in at least one category).
- Every category should be accompanied by clear and unambiguous classification criteria defining what specimens are to be put in that category.
- The taxonomy should be comprehensible and useful not only to experts in security but also to users and administrators with less knowledge and experience of security.
- The terminology of the taxonomy should comply with the established security terminology.

He also took into account the properties that had been previously identified by Amoroso [2] which include:

- Completeness. The taxonomy should encompass all possible attacks on the target system.
- Appropriateness. The selected taxonomy should appropriately characterize the attacks to the target system; that is any constraints on the taxonomy or on the system should be specified and considered before application.

Attack taxonomy should differentiate attacks that require insider access to a system from those that can be initiated by external intruders who may not have gained access to the system. Based on his research, and his analysis of previous attempts to develop classifications, Lindqvist [105] decided to use the traditional aspects of computer security: Confidentiality, Integrity and Availability (CIA) as a basis for his model. From this, he developed two classification schemes as noted in the tables below. One classification focused on intrusion technique, the other on intrusion result.

Table 3. Taxonomy of Intrusions: Intrusion Technique [105]

Category		
NP5: Bypassing intended controls	Password Attacks	Capture
		Guessing
	Spoofing Privileged Programs	
	Utilizing weak authentication	
NP6: Active misuse of resources	Exploiting inadvertent write permissions	
	Resource exhaustion	
NP7: Passive misuse of resources	Manual browsing	
	Automated searching	Using a personal tool
		Using a publicly available tool

Table 4. Taxonomy of Intrusions: Intrusion Result [105]

Category		
Exposure	Disclosure of confidential information	Only user information disclosed
		System (and user) information disclosed
	Service to unauthorized entities	Access as an ordinary user account
		Access as a special system account
		Access as client root
	Access as server root	
Denial of service	Selective	Affects a single user at a time
		Affects a group of users
	Unselective	Affects all users of the system
	Transmitted	Affects all users of other systems
Erroneous output	Selective	Affects a single user at a time
		Affects a group of users
	Unselective	Affects all users of the system
	Transmitted	Affects all users of other systems

Lodin [108] further distinguishes intrusions by who is doing the intruding. He classifies potential intruders into two types [77-80]:

1. Outside Intruders - This is the most publicized form of intruder and receives the bulk of attention during security implementations. Typical terms used to identify outside intruders are hacker and cracker.
2. Inside Intruders - Studies by the Computer Security Institute in conjunction with the FBI have revealed that most intrusions and attacks come from within an organization and result from an authorized user maliciously invoking an

authorized process or by manipulating a known vulnerability. This type of intrusion has the potential for causing the greatest damage to the organization.

Finally Sundaram [179] believes that it is important to also consider the type of intrusion, regardless of the source. He divides intrusion into 6 main types:

1. Attempted break-ins, which are detected by atypical behavior profiles or violations of security constraints.
2. Masquerade attacks which are detected by atypical behavior profiles or violations of security constraints.
3. Penetration of the security control system, which are

detected by monitoring for specific patterns of activity.

4. Leakage, which is detected by atypical use of system resources.
5. Denial of service, which is detected by atypical use of system resources.
6. Malicious use, which is detected by atypical behavior profiles, violations of security constraints, or use of special privileges.

2.2 Intrusion Threat

Enterasys [39] Networks identified five reasons why the threat of intrusion detection should be taken seriously.

1. The threat is real: The amount of unauthorized information security events rose in 2000. A staggering 70% of organizations reported a security incident. This figure is up from 42% reported in 1996.
2. Everything is on the net: Many companies have migrated key information and business resources to the Internet. This has exposed sensitive corporate information.
3. Firewalls and VPNs are not enough: Although correct firewall policy can

minimize the exposure of many networks, hackers are evolving their attacks and network subversion methods. These techniques include e-mail based Trojan horses, stealth scanning techniques and actual attacks, which bypass firewall policies by tunneling access over allowed protocols such as ICMP or DNS.

4. The amount of new vulnerabilities is increasing: The amount of information on network vulnerabilities is so pervasive, many companies are selling now subscriptions to vulnerability digests, automatically tailored to a company's profile of operating systems and network hardware. Vulnerabilities are also showing up in security equipment, such as firewalls and even IDS equipment.
5. Hackers are getting smarter: Hackers can use port scanners to attempt to connect to a target machine on every port and build a list of potential active ports. Modern port scanners include operating system identification, can target entire ranges of IP addresses and even send in decoy scans to make it more difficult for the target to identify who the scanner source really is. Figure 1 shows the sophistication of hackers' tools over time.

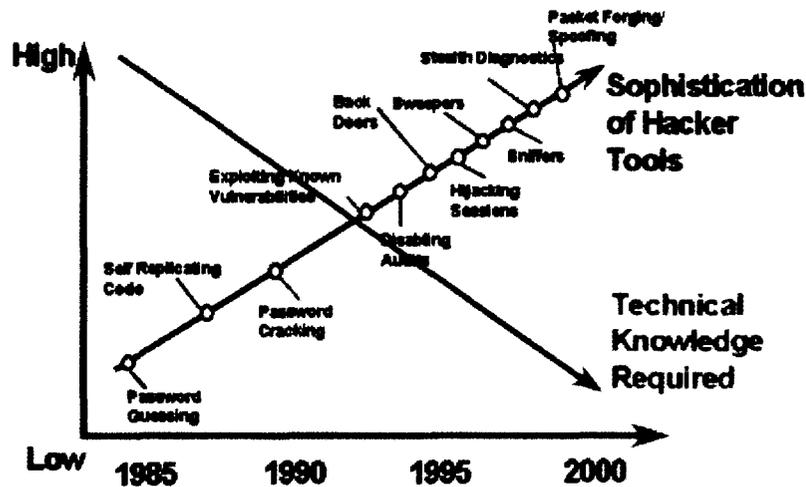


Figure 1. Sophistication of Hacker Tools [39, 179]

2.3 Intrusion Attacks

Enterasys Networks [39] is one of the sources warning us of the extensive occurrence of network intrusion. Mahoney [117, 118] notes that:

The rate of computer intrusions is approximately doubling each year, consistent with the overall growth of the Internet. The Computer Emergency Response Team (CERT) reported 3734 incidents in 1998, 9859 in 1999 and 8836 in the first 6 months of 2000. In a recent audit of U.S. federal agencies by the GAO [39] investigators were able to pierce security at nearly every system they tested.

2.4 Intrusion Defense

Denning [31-33] noted that there were four factors serving as motivation for the development of intrusion detection and defense systems:

1. Most existing systems have security flaws that render them susceptible to intrusions, penetrations, and other forms of abuse; finding and fixing all these deficiencies is not feasible for technical and economic reasons;
2. Existing systems with known flaws are not easily replaced by systems that are more secure-mainly because the systems have attractive features that are missing in the more-secure systems, or else they cannot be replaced for economic reasons;
3. Developing systems that are absolutely secure is extremely difficult, if not generally impossible; and
4. Even the most secure systems are vulnerable to abuses by insiders who misuse their privileges.

3. Intrusion Detection Systems (IDS): Models and Methods

Sundaram [179], Jackson [76-79], Anderson [3], Bace [10], Bishop [14-16], Eskin [41-44] and others [12, 46, 64, 86,97] have advanced various research efforts in the area of intrusion detection systems, models and methods. These efforts include the following:

1. Generic Intrusion Detection Model
2. NSM (Network Security Monitor) Model
3. Autonomous Agents Model
4. Behavior-based Intrusion Detection Model
5. Predictive Pattern Generation Model
6. Knowledge-based Intrusion Detection Model

4. Intrusion Detection Systems: Implementation and Integration

4.1 Host-based

Zirkle [207] described host-based IDS as "loading a piece of software on the system to be monitored". This software, which is generally defined as either host wrappers/personal firewalls or agent-based software, performs the following:

- Uses log files and/or the system's auditing agents as sources of data.
- Looks at the communications traffic in and out of a single computer;
- Checks the integrity of system files, and watches for suspicious processes, including changes to system files and user privileges.

Host-based detection software is particularly effective in detecting trusted-insider attacks ("anomalous activity"). One drawback for host-based intrusion detection is that the software must be installed on each computer on the network to be protected.

4.2 Network-based

Northcutt [138-139] described network-based intrusion detection system (NIDS) as an ID system that monitors the traffic on its network

segment as a data source. Implementation requires:

- The network interface card is placed in promiscuous mode to capture all network traffic that crosses its network segment; and
- A sensor, which monitors packets traveling on that network segment.

The objective is to determine if packet flow matches a known signature. There are three signatures that are particularly important:

1. String signatures that look for a text string that indicates a possible attack,
2. Port signatures simply watch for connection attempts to well known, frequently attacked ports, and
3. Header signatures that watch for dangerous or illogical combinations in packet headers.

5. Intrusion Detection Systems: Hybrid Implementations

5.1 Firewalls

Graham [53] describes the role of firewalls, and to what extent, if any, a firewall may be a NIDS, or has a cooperative relationship with NIDS.

He notes that it is simply not true that firewalls recognize attacks and block them. Firewalls are really just rule-based systems that allow/deny traffic passing through them.

5.2 Bastion Hosts

A bastion host is a computer that is fully exposed to attack.

The goal is to ensure that there is a minimal chance that an attack will actually penetrate the bastion host

5.3 Honeypots

Honeypots are designed to look like something that an intruder can hack. Some examples include [53]:

- Installing a machine on the network with no particular purpose other than to log all attempted access.

- Install special software designed for this purpose. It has the advantage of making it look like the intruder is successful without really allowing them access.

6. Placement of IDS

Placement of IDS/NIDS can take any of the following forms [53]:

1. NIDS can be placed on hosts (in non-promiscuous mode) which are otherwise defenseless, e.g., Windows 98, and are not capable of creating logs that might be processed by a host-based system
2. IDS is most effective on the network perimeter, such as on both sides of the firewall, near the dial-up server, and on links to partner networks.
3. NIDS can be placed on the corporate WAN backbone where it can monitor packet traffic attempting to enter the network.
4. For server farms, One solution may be to isolate critical servers to their own network segment, and dedicate a specialized NIDS to monitor that segment.

7. Intrusion Detection Systems: Implementation Strategies

Graham [53] notes six implementation strategies to consider

1. Put firewalls between areas of the network with different security requirements (i.e. between internet-localnet, between users-servers, between company-partners, etc).
2. Use network vulnerability scanners to double check firewalls and to find holes that intruders can exploit.
3. Use host policy scanners to make sure they conform to accepted practices (i.e. latest patches).
4. Use Network intrusion detection systems and other

- packet sniffing utilities to see what is actually going on.
5. Use host-based intrusion detection systems and virus scanners to flag successful intrusions.

8. Intrusion Detection Systems: Evaluation Criteria

An intrusion detection system should address the following issues, regardless of what mechanism it is based on [11, 53, 77, 108]

1. It should support, not interfere with the security policies and the business operations of the organization.
2. It must run continually without human supervision.
3. It must be fault tolerant in the sense that it must survive a system crash and not have its knowledge base rebuilt at restart.
4. It must resist subversion.
5. It must impose minimal overhead on the system.
6. It must observe deviations from normal activity.
7. It must be easily customized to the system in question.
8. It must cope with changing system behavior over time as new applications are being added.
9. It must be difficult to fool even with full knowledge of internal workings by attackers.

9. Conclusion

The threat and actuality of intrusion is real. More often than not, organizations are not prepared to protect themselves from intrusions. However, each organization should have a security policy and a strategy to combat intrusion efficiently and effectively. The strategy should include preparation, monitoring, detection, recovery and response. If this is implemented, organizations will be able to protect their systems, networks and their sensitive data.

10. Acknowledgments

The work described in this paper was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under contract with the National Aeronautics and Space Administration (NASA).

Concerning the reference list we have tried to be reasonably complete; however, those articles which were not included were considered not to bear directly on the topics of this review or were inadvertently overlooked. We apologize to both the researchers and readers if we have omitted any relevant article.

REFERENCES:

- [1] Allen, J., Christie, A., Fithin, W., McHugh, J., Pickel, J., and E. Stoner, "State of the Practice of Intrusion Detection Technologies." (CMU/SEI-99/TR-028). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2000.
- [2] Amoroso, E.G. "Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Trace Back, Traps and Response." *Intrusion.net*, 1999.
- [3] Anderson, D.; Frivold, T.; and A. Valdes, "Next-generation Intrusion Detection Expert System (NIDES)", Technical report, SRI-CSL-95-07, SRI International, Computer Science Lab, 1995.
- [4] Anderson, R. and A. Khattak, "The Use of Information Retrieval Techniques for Intrusion Detection", *Proceedings of RAID*, Louvain-la-Neuve, Belgium, 1998.
- [5] Anderson, R. "Liability and Computer Security: Nine Principles." Third European Symposium on Research in Computer Security, Brighton, U.K., November 1994.
- [6] Anderson, J. P. "Computer Security Threat Monitoring and Surveillance." Technical Report, James P Anderson Co., Fort Washington, Pennsylvania, 1980.
- [7] Apap, F., A. Honig, S. Hershkop, E. Eskin, and S. Stolfo. "Detecting malicious software by monitoring anomalous windows registry accesses." Technical report, CUCS, 2001.
- [8] Autonomous Agents. Technical Report CSD-TR-95-022, Department of Computer Sciences, Purdue University, 1995.
- [9] Axelsson, S., "On a Difficulty of Intrusion Detection." *Proc. of the Second International Workshop on Recent Advances in Intrusion Detection*, W. Lafayette, IN, 1999.
- [10] Bace, Rebecca, "Intrusion Detection." Macmillan Tech. Pub. Indianapolis, IN, 2000.
- [11] Bace, Rebecca, "A New Look at Perpetrators of Computer Crime." *Proc. Sixteenth Department of Energy Computer Security Group Conference*, Denver, CO, 1994.
- [12] Balasubramaniyan, J.S., J. O. Garcia-Fernandez, D. Isacoff, E.H. Spafford, and D. Zamboni. "An Architecture for Intrusion Detection Using Autonomous Agents." COAST technical report 98/05, Purdue University, W. Lafayette, IN, 1998.
- [13] Bauer, D. and M.E. Koblenz. "NIDX—An Expert System for Real-Time Network Intrusion Detection." *Proceedings of the IEEE Computer Networking Symposium*, New York, NY, 98-106, 1998.
- [14] Bishop, M., "A Standard Audit Log Format." *Proceedings of the 1995 National Information Systems Security Conference*, Baltimore, MD, 1995.
- [15] Bishop, M., "Vulnerabilities Analysis: Extended Abstract." *Proceedings of the Second International Workshop on Recent Advances in Intrusion Detection*, W. Lafayette, IN, 1999.
- [16] Bishop, M. "A Model of Security Monitoring." *Proceedings of the Fifth Annual Computer Security Applications Conference*, Tucson, AZ, 1989.
- [17] Blain, L. and Y. Deswarte. "An Intrusion-Tolerant Security Server for an Open Distributed System." *Proceedings of the European Symposium on Research in Computer Security*, Toulouse, France, 1990.
- [18] Brentano, J. "An Expert System for Detecting Attacks on Distributed Computer Systems." Master thesis, Division of Computer Science, University of California, Davis, CA, March 1991.
- [19] Carnegie Mellon Software Engineering Institute, "State of the Practice of Intrusion Detection Technologies," Technical Report, CMU/SEI-99-TR-028, ECS-99-028, 2000.
- [20] Carrettoni, F., S. Castano, G. Martella, and P. Samarati. "RETISS: A Real Time Security System for Threat Detection Using Fuzzy Logic." *Proceedings of the Twenty-Fifth Annual IEEE International Carnahan Conference on Security Technology*, Taipei, Taiwan, 1991.
- [21] Cedex, CS. Genetic Algorithms, an Alternative Tool for Security Audit Trails Analysis. *Lodovic Me, SUPELEC, France, 1993.*
- [22] Cheung, S., R. Crawford, M. Dilger, J. Frank, J. Hoagland, K. Levitt, J. Rowe, S. Staniford-Chen, R. Yip, and D. Zerkle. "The Design of GridS: A Graph-Based Intrusion Detection System." University of California, Davis, Computer Science Department technical report CSE-99-2, 1999.
- [23] Cheung, S. and K. N. Levitt. "Protecting Routing Infrastructures from Denial of Service Using Cooperative Intrusion Detection." *Proceedings New Security Paradigms Workshop*, Cumbria, U.K., 1997.
- [24] Corbitt, T. "The Computer Misuse Act," *Computer Fraud and Security Bulletin*, 13-17, 1994.
- [25] Crosbie, M. "Applying Genetic Programming to Intrusion Detection." *Proceedings of AAAI Fall Symposium on Genetic Programming*, San Jose, CA, 1995.

- [25] Crosbie, M. and E. Spafford. Defending a Computer System Using Autonomous Agents." *Proceedings of the Eighteenth National Information Systems Security Conference*, Baltimore, MD, 1995.
- [26] Debar, H., M. Becker, and D. Siboni. "A Neural Network Component for an Intrusion Detection System." *Proceedings of the IEEE Symposium on Research in Security and Privacy*, Oakland, CA 1992.
- [27] Debar, H., M. Ludovic, and S. Felix Wu (eds.), "Recent Advances in Intrusion Detection," *Third International Workshop, Raid 2000*, Toulouse, France. Springer Verlag, 2000.
- [28] DeDios, P., R. El-Khalil, K. Sarantakos, M. Miller, E. Eskin, W. Lee, and S. Stolfo. "Heuristic audit of network traffic: A data mining-based approach to network intrusion detection." Technical report, Columbia University, CUCS, 2001.
- [29] Denmac Systems "Network Based Intrusion Detection," Denmac Systems, Inc., 1999.
- [30] Denning, D. and P. Neumann. *Requirements and Model for IDES—A Real-Time Intrusion Detection Expert System, Final Report*, Computer Science Laboratory, SRI International, 1985
- [31] Denning, D. "An Intrusion Detection Model." *IEEE Transactions on Software Engineering*, 13, 2, 222-232, 1967.
- [32] Denning, D., D. Edwards, R. Jagannathan, T. Lunt, P. Neumann. "A Prototype IDES: A Real-Time Intrusion Detection Expert System." Computer Science Laboratory, SRI International, 1987.
- [33] Dias, G., K.N. Levitt, and B. Mukherjee. "Modeling Attacks on Computer Systems: Evaluating Vulnerabilities and Forming a Basis for Attack Detection." *SRI Intrusion Detection Workshop*, Menlo Park, CA, 1990.
- [34] Didier, S., and R. Molva, "IDAMN: An Intrusion Detection Architecture for Mobile Networks", *IEEE Journal on Selected Areas in Communications*, 15, 7, 1997.
- [35] Doak, J., "Intrusion Detection: The Application of Feature Selection, a Comparison of Algorithms, and the Application of a Network Analyzer." Master thesis, University of California, Davis, CA, 1992.
- [36] Dowell, C. and P. Ramstedt. "The Computer watch Data Reduction Tool." *Proceedings of the Thirteenth National Computer Security Conference*, Washington, DC, 1990.
- [37] Dunigan, T. and Hinkel, G. "Intrusion Detection and Intrusion Prevention on a Large Network: A Case Study." *Proceedings 1st Workshop on Intrusion Detection and Network Monitoring*. Santa Clara, CA 1999.
- [38] Enterasys Networks, "Intrusion Detection System: Hackers Are Getting Smarter". *Enterasys Networks*. 2001
- [39] Escamilla, T. "Intrusion Detection: Network Security Beyond the Firewall." John Wiley and Sons, 1998.
- [40] Eskin, E. "Anomaly detection over noisy data using learned probability distributions." In *Proceedings of ICML 2000*, Menlo Park, CA, 2000.
- [41] Eskin, E., A. Arnold, M. Prerau, L. Portnoy, and S. Stolfo. "A geometric framework for unsupervised anomaly detection: Detecting intrusions in unlabeled data." Technical report, CUCS, 2002.
- [42] Eskin, E., M. Miller, Z.D. Zhong, G. Yi, W. Lee, S. Stolfo. "Adaptive Model Generation for Intrusion Detection Systems." *Workshop on Intrusion Detection and Prevention, 7th ACM Conference on Computer Security*, 2001.
- [43] Eskin, E., W. Lee, and S. Stolfo. Modeling system calls for intrusion detection with dynamic window sizes. In *Proceedings of DARPA Information Survivability Conference and Exposition II (DISCEX II)*, Anaheim, CA, 2001.
- [44] Fan, W. and S. Stolfo, "Ensemble-Based Adaptive Intrusion Detection," *Proceedings SIAM Int. Conference on Data Mining*, Arlington, VA. 2002.
- [45] Fan, W., Lee, W.; Stolfo, S. and M. Miller, "A Multiple Model Cost-Sensitive Approach for Intrusion Detection" *Eleventh European Conference on Machine Learning*, 2000.
- [46] Feiertag, R., L. Benzinger, S. Rho, and S. Wu. "Intrusion Detection Intercomponent Adaptive Negotiation." *Proceedings of the Second International Workshop on Recent Advances in Intrusion Detection*, W. Lafayette, IN, 1999.
- [47] Forte, D. "Intrusion Detection Systems" *login*: 24, 1, 1999.
- [48] Frank, J., "Machine Learning and Intrusion Detection: Current and Future Directions." *Proceedings of the Seventeenth National Computer Security Conference*, Baltimore, MD, 1994.
- [49] Frincke, D., D. Tobin, and Y. Ho. "Planning, Petri Nets, and Intrusion Detection." *Proceedings of Twenty-First National Information System Security Conference*, Crystal City, VA, 1998.
- [50] Garvey, T. and T. Lunt. "Model-Based Intrusion Detection." *Proceedings of the Fourteenth National Computer Security Conference*, Washington, DC, 1991.
- [51] Ghosh, A. and A. Schwartzbard. "A study in using neural networks for anomaly and misuse detection." In

Proceedings of the Eighth USENIX Security Symposium, 1999.

- [52] Graham, R., "FAQ: Network Intrusion Detection Systems," *InfoWorld*, Robert Graham. 1998-2000.
- [53] Gross, A., "Analyzing Computer Intrusions." Ph.D. thesis, University of California, San Diego, Department of Computer Sciences, San Diego, CA, 1997.
- [54] Habra, N., B. Le Charlier, and A. Mounji. "Advanced Security Audit Trail Analysis on UNIX: Implementation Design of the NADF Evaluator." Research report, Universitaires Notre Dame de la Paix, Namur, Belgium, 1993.
- [55] Habra, N., B. Le Charlier, and A. Mounji. "Preliminary Report on Advanced Security Audit Trail Analysis on UNIX." Universitaires Notre Dame de la Paix, Namur, Belgium, Research report, 1991.
- [56] Halme, L. and B. Kahn. "Building a Security Monitor with Adaptive User Work Profiles." *Proc., 11th National Computer Security Conference*, 1988.
- [57] Halme, L. and R.K. Bauer. "AINT Misbehaving—A Taxonomy of Anti-intrusion Techniques." *Proceedings of the Eighteenth National Information Systems Security Conference*, Baltimore, MD, 1995.
- [58] Heady, R., G. Luger, A.B. Maccabe, and M. Servilla. "The Architecture of a Network Level Intrusion Detection System." Technical report CS90-20, Department of Computer Science, University of New Mexico, Albuquerque, NM, 1990.
- [59] Heberlein, L, B. Mukherjee and K. Levitt. "Internetwork Security Monitor: An Intrusion Detection System for Large-scale Networks." *Proceedings of the 15th National Computer Security Conference*, 1992.
- [60] Heberlein, L., G. Dias, K. Levitt, B. Mukherjee, J. Wood and D. Wolber. "A Network Security Monitor." *Proceedings of the IEEE Symposium on Research in Security and Privacy*, 1990.
- [61] Heberlein, T., K. Levitt and B. Mukherjee. "A Method to Detect Intrusive Activity in a Networked Environment." *Proceedings of the 14th National Computer Security Conference*, 1991.
- [62] Heberlein, T., "Network Security Monitor (NSM)--Final Report." Lawrence Livermore National Laboratory, Davis, CA, 1995.
- [63] Heberlien, T., B. Mukherjee, K.N. Levitt; G. Dias and D. Mansur. "Towards Detecting Intrusions in a Networked Environment." *Proceedings of the Fourteenth Department of Energy Computer Security Group Conference*, 1991.
- [64] Helman, P. and G. Liepins. "Statistical Foundations of
- [65] Helman, P., G. Liepins, and W. Richards. "Foundations of Intrusion Detection." *Proceedings of the Fifth Computer Security Foundations Workshop*, Franconia, NH, 1992.
- [66] Hershkop, S., F. Apap, E. Glanz, T. D'alberti, E. Eskin, Sal Stolfo, and J. Lee. "Hobids: A data mining approach to host based intrusion detection." Technical report, CUCS, 2001.
- [67] Herve, D. "What is behavior-based intrusion detection?" IBM Zurich Research Laboratory. SANS Institute Resources, *Intrusion Detection FAQ*, 2000.
- [68] Hochberg, J., K. Jackson, C. Stallings, J.F. McClary, D. DuBois, and J. Ford. "NADIR: An Automated System for Detecting Network Intrusion and Misuse." *Computers and Security* 12, 3, 235-248, 1993.
- [69] Hofmeyer, S.A., S. Forrest, and A. Somayaji. "Intrusion detection using sequences of system calls," *Journal of Computer Security*, 6:151-180, 1998.
- [70] Hubbard, B., T. Haley, N. McAuliffe, L. Schaefer, N. Kelem, D. Wolcon, R. Feiertag and M. Schaefer. *Computer System Intrusion Detection*. Trusted Information Systems, Inc. TIS Report No.348, 1990
- [71] Ilgun, K. "USTAT - A Real-time Intrusion Detection System for UNIX." Master's Thesis, University of California at Santa Barbara, 1992.
- [72] Ilgun, K., R.A. Kemmerer, and P. Porras. "State Transition Analysis: A Rule-Based Intrusion Detection Approach." *IEEE Transactions on Software Engineering* 21, 3, 181-199, 1995.
- [73] Ilgun, K., R.A. Kemmerer, and P.A. Porras. "State transition analysis: A rule-based intrusion detection approach." *IEEE Transactions on Software Engineering*, 21, 3, 181-199,1995.
- [74] Ilgun, K. "USTAT: A Real-Time Intrusion Detection System for UNIX." Master thesis, University of California, Santa Barbara, CA, 1992.
- [75] Jackson, K. A., "Intrusion Detection System (IDS) Product Survey". Published by *Distributed Knowledge Systems Team; Computer Research and Applications Group; Computing, Information and Communications Division*; Los Alamos National Laboratory, Los Alamos, New Mexico, 1999.
- [76] Jackson, K., D. DuBois and C. Stallings. "A Phased Approach to Network Intrusion Detection." *Proceedings of the United States Department of Energy Computer Group Conference*, 1991.

- [77] Jackson, K., D. DuBois, and C. Stallings, "An Expert System Application for Network Intrusion Detection," *Proceedings of the 14th Department of Energy Computer Security Group Conference*, Washington, DC, 1991.
- [78] Jackson, K., M.C. Neumann, D. Simmonds, C. Stallings, J. Thompson, and G. Christoph. "An Automated Computer Misuse Detection System for UNICOS." *Proceedings of the Cray Users Group Conference*, Tours, France, 1994.
- [79] Javitz, H. and A. Valdes, "The SRI IDES Statistical Anomaly Detector," Proc. IEEE Symposium on Security and Privacy, Oakland, CA, 1991.
- [80] Kim, G. and E. H. Spafford. "Tripwire: A Case Study in Integrity Monitoring." *Internet Besieged: Countering Cyberspace Scofflaws*, edited by Dorothy and Peter Denning, Addison-Wesley, 1997.
- [81] Ko, C., G. Fink, and K. Levitt. "Automated detection of vulnerabilities in privileged programs by execution monitoring." In *Proceedings of the 10th Annual Computer Security Applications Conference*, 134-144, 1994.
- [82] Kossakowski, P., "Responding to Intrusions." (CMU/SEI-SIM-006). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1999.
- [83] Kumar, S. "Classification and Detection of Computer Intrusions." PhD Dissertation, Purdue University, W. Lafayette, IN, 1995.
- [84] Kumar, S. and E. Spafford. "A Pattern Matching Model for Misuse Intrusion Detection." *Proceedings of the Seventeenth National Computer Security Conference*, Baltimore, MD, 1994.
- [85] Kumar, S. and E. Spafford. "A software architecture to support misuse intrusion detection." In *Proceedings of the 18th National Information Security Conference*, 194-204, 1995.
- [86] Lane, T. and C. Brodley. "An Application of Machine Learning to Anomaly Detection." *Proceedings of the Twentieth National Information System Security Conference*, Baltimore, MD, 1997.
- [87] Lane, T. and C. E. Brodley, "Sequence Matching and Learning in Anomaly Detection for Computer Security," *AAAI Workshop: Approaches to Fraud Detection and Risk Management*, 43-49, 1997.
- [88] Lankewicz, L. and M. Benard. "Real-Time Anomaly Detection Using a Nonparametric Pattern Recognition Approach." *Proceedings of the Seventh Computer Security Applications Conference*, San Antonio, TX, 1991.
- [89] Lankewicz, L. and M. Bernard. "A Nonparametric Pattern Recognition Approach to Intrusion Detection." Technical report TUTR 90-106, Tulane University Department of Computer Science, New Orleans, LA, 1990.
- [90] Lee, W. "A Data Mining Framework for Constructing Features and Models for Intrusion Detection Systems." PhD Thesis, Columbia University, 1999.
- [91] Lee, W. and D. Xiang. "Information-theoretic measures for anomaly detection." In *Proceedings of the 2001 IEEE Symposium on Security and Privacy*, 2001.
- [92] Lee, W. and S. Stolfo, "Data Mining Approaches for Intrusion Detection" *Proceedings, Seventh USENIX Security Symposium*, San Antonio, TX, 1998.
- [93] Lee, W., and S.J. Stolfo. "Combining Knowledge Discovery and Knowledge Engineering to Build IDSs." *Proceedings of the Second International Workshop on Recent Advances in Intrusion Detection*, W. Lafayette, IN, 1999.
- [94] Lee, W., Miller, M., Stolfo, S. Jallad, K. Park, C. Zadok, E. and V. Prabhakar, "Toward Cost-Sensitive Modeling for Intrusion Detection" Columbia University Computer Science Technical Report CUCS-002-00, 2000.
- [95] Lee, W., Park, C. and S. Stolfo, "Towards Automatic Intrusion Detection using NFR" *Proceedings 1st USENIX Workshop on Intrusion Detection and Network Monitoring*, 1999.
- [96] Lee, W., S. Stolfo, K. Mok. "Mining Audit Data to Build Intrusion Detection Models." *Proceedings of the Fourth International Conference on Knowledge Discovery and Data Mining*, 1998.
- [97] Lee, W., S. Stolfo, P.K. Chan, E. Eskin, W. Fan, M. Miller, S. Hershop, J. Zhang. "Real Time Data Mining-based Intrusion Detection." *Proceedings of DISCEX II*, 2001.
- [98] Lee, W., S.J. Stolfo, and K Mok. "Data mining in work flow environments: Experiences in intrusion detection." *Proceedings of the Conference in Knowledge Discovery and Data Mining*, 1999.
- [99] Lee, W., S.J. Stolfo, and K. W. Mok. "A Data Mining Framework for Building Intrusion Detection Models." *Proceedings of the Twentieth IEEE Symposium on Security and Privacy*, Oakland, CA 1999.
- [100] Lee, W., S.J. Stolfo, and P.K. Chan. "Learning patterns from Unix processes execution traces for intrusion detection." *Proceedings of the AAAI-97 Workshop on AI Approaches to Fraud Detection and Risk Management*, 50-56. Menlo Park, CA: AAAI Press, 1997.
- [101] Levitt, K. (ed.), "Proceedings of Workshop on Future Directions In Computer Misuse and Anomaly Detection." University of California, Davis, CA, 1992.

- [102] Liepins, G. and H.S. Vaccaro. "Anomaly Detection: Purpose and Framework." *Proceedings of the Twelfth National Computer Security Conference*, Washington, DC, 1989.
- [103] Liepins, G. and H.S. Vaccaro. "Intrusion Detection: Its Role and Validation." *Computers and Security*, 11, Oxford, UK: Elsevier Science Publishers, Ltd., 347-355, 1992.
- [104] Lindquist, U., and E. Jonsson, "How to Systematically Classify Computer Security Intrusions" *Proceedings IEEE Symposium Research in Security and Privacy*, Oakland, CA 1997.
- [105] Lippmann, R., J.W. Haines, D.J. Fried, J. Korba, K. Das. The 1999 DARPA Off-Line Intrusion Detection Evaluation. *Computer Networks*, 34, 579-595, 2000.
- [106] Lippmann, R.; Fried, D.; Graf, I.; Haines, J.; Kendall, K.; McClung, D.; Weber, D.; Webster, S.; Wyschogrod, D.; Cunningham, R.; and M. Zissman, "Evaluating Intrusion Detection Systems: The 1998 DARPA Off-Line Intrusion Detection Evaluation," *Proceedings DARPA Information Survivability Conference*, 2000.
- [107] Lodin, S., "Intrusion Detection Product Evaluation Criteria," Ernst & Young LLP, [Hyperlink: docshow.net/ids.htm](http://docshow.net/ids.htm), 1998.
- [108] Lundin, E. and E. Jonsson. "Privacy versus Intrusion Detection "Analysis." *Proceedings of the Second International Workshop on Recent Advances in Intrusion Detection*, W. Lafayette, IN, 1999.
- [109] Lunt, T. "Automated Audit Trail Analysis and Intrusion Detection: A Survey." *Proceedings of the Eleventh National Computer Security Conference*, Washington, DC, 1988.
- [110] Lunt, T. "A survey of intrusion detection techniques." *Computers and Security*, 12, 405-418, 1993.
- [111] Lunt, T. "Detecting intruders in computer systems." In *Proceedings of the Conference on Auditing and Computer Technology*, 1993.
- [112] Lunt, T. and R. Jagannathan. "A Prototype Real-Time Intrusion Detection Expert System." *Proceedings of the 1988 IEEE Symposium on Security and Privacy*, Oakland, CA, 1988.
- [113] Lunt, T., "Real-Time Intrusion Detection." *Proceedings of COMPCON Spring '89*, San Francisco, CA, 1989.
- [114] Lunt, T. "Knowledge-Based Intrusion Detection." *Proceedings of the AI Systems in Government Conference*, Washington, DC, 1989.
- [115] Lunt, T., Tamaru, F. Gilham, R. Jagannathan, P. Neumann, H. Javitz, A. Valdes, and T. Garvey. "A real-time intrusion detection expert system (IDES) – final technical report." Computer Science Laboratory, SRI International, Menlo Park, California, 1992.
- [116] Mahoney, M. and P. Chan. "Detecting novel attacks by identifying anomalous network packet headers." Technical Report CS-2001-2, Florida Institute of Technology, Melbourne, FL, 2001.
- [117] Mahoney, M., "Computer Security: A Survey of Attacks and Defenses" Hyperlink: docshow.net/ids.htm, 2000.
- [118] Maiwald, E., "Automating Response to Intrusions." *The Fourth Annual UNIX and NT Network Security Conference*. Orlando, FL: The SANS Institute, 1998.
- [119] Mandanaris, S., M. Christensen, D. Zerkle, and K. Hermis. "A Data Mining Analysis of RTID Alarms." *Proceedings of the Second International Workshop on Recent Advances in Intrusion Detection*, W. Lafayette, IN, 1999.
- [120] Mansfield, G. K. Ohta, Y. Takei, N. Kato, and Y. Nemoto. "Towards Trapping Wily Intruders in the Large." *Proceedings of the Second International Workshop on Recent Advances in Intrusion Detection*, W. Lafayette, IN, 1999.
- [121] Marceau, C. "Characterizing the behavior of a program using multiple-length n-grams." In *Proceedings of the New Security Paradigms Workshop*, 2000.
- [122] Marchette, D. "Computer Intrusion Detection and Network Monitoring: A Statistical Viewpoint." Springer Verlag, 2001.
- [123] Mark, G. "Intrusion Detection," *Software Technology Review*, Software Engineering Institute. Carnegie Mellon University, 2000.
- [124] McAuliffe, N., D. Wolcott, L. Schaefer, N. Kelem, B. Hubbard, and T. Haley. "Is Your Computer Being Misused? A Survey of Current Intrusion Detection Technology." *Proceedings of the Sixth Annual Computer Security Applications Conference*, Tucson, AZ, 1990.
- [125] McConnell, J., D.A. Frincke, D. Tobin, J. Marconi, and D. Polla. "A Framework for Cooperative Intrusion Detection." *Proceedings of Twenty-First National Information System Security Conference*, Crystal City, VA, 1998.
- [126] Me' L. "GASSATA, a Genetic Algorithm as an Alternative Tool for Security Audit Trails Analysis." *First International Workshop on the Recent Advances in Intrusion Detection*, Louvain-la-Neuve, Belgium, 1998.
- [127] Me, Ludovic. "Security Audit Trail Analysis Using Genetic Algorithms." *Proceedings of the Twelfth International Conference on Computer Safety, Reliability, and Security*, Poznan, Poland, 1993.
- [128] Mell, P. and M. McLarnon. "Mobile Agent Attack Resistant Distributed Hierarchical Intrusion Detection

- Systems." *Proceedings of the Second International Workshop on Recent Advances in Intrusion Detection*, W. Lafayette, IN, 1999.
- [129] Miller, M. "Learning Cost-Sensitive Classification Rules for Network Intrusion Detection Using RIPPER." Technical Report CUCS-035-99, Columbia University, 1999.
- [130] MIT Lincoln Labs. 1999 DARPA intrusion detection evaluation. In <http://www.ll.mit.edu>, 1999.
- [131] Moitra, A., "Real-Time Audit Log Viewer and Analyzer." *Proceedings of the Fourth Workshop on Computer Security Incident Handling*, Denver, CO, 1992.
- [132] Mounji, A. "Languages and Tools for Rule-Based Distributed Intrusion Detection." Thesis, Faculte's Universitaires Notre-Dame de la Paix, Namur, Belgium, 1997.
- [133] Mukherjee, B.; Heberlein, L. T. and K.N Levitt. "Network Intrusion Detection," *IEEE Network*, 8, 3, 26-41, 1994.
- [134] Neumann, P. G., and P. A. Porras "Experience with EMERALD to Date", *SRI International, 1st USENIX Workshop on Intrusion Detection and Network Monitoring*. Santa Clara, California, 73-80, 1999.
- [135] Neumann, P. G. and D.B. Parker. "A Summary of Computer Misuse Techniques." *Proceedings of the Twelfth National Computer Security Conference*, 1989.
- [136] Northcutt, S., "What is Network Based Intrusion Detection?" SANS Institute. SANS Institute Resources, *Intrusion Detection FAQ*, Hyperlink: ID FAQ, 2000.
- [137] Northcutt, S. "Network Intrusion Detection: An Analyst's Handbook." Indianapolis, IN: New Rider, 1999.
- [138] Northcutt, S. "What the Hackers Know about You." SANS Institute. SANS Institute Resources, *Intrusion Detection FAQ*, Hyperlink: ID FAQ, 1999.
- [139] Ong, T.H., C.P. Tan, Y.T. Tan, C.K. Chew, and C. Ting. "SNMS—Shadow Network Management System." *Proceedings of the Second International Workshop on Recent Advances in Intrusion Detection*, W. Lafayette, IN, 1999.
- [140] Panagiotis, A. "Intrusion Detection Systems". *Daemon News*. May 1999.
- [141] Paxson, V. "Bro: A system for detecting network intruders in real-time." In *Proceedings of the 7th USENIX Security Symposium*, San Antonio, TX, 1998.
- [142] Paxson, V. and M. Handley. "Defending Against Network IDS Evasion." *Proceedings of the Second International Workshop On Recent Advances in Intrusion Detection*, W. Lafayette, IN, 1999.
- [143] Piccioto, Jeffrey. "The Design of an Effective Auditing Subsystem." *Proceedings of the 1987 IEEE Symposium on Security and Privacy*, Oakland, CA, 1987.
- [144] Pichnarczyk, K.; Weeber, S.; and Feingold, R. "Unix Incident Guide: How to Detect an Intrusion." (CIAC-2305 R.1) Lawrence Livermore National Laboratory, Department of Energy Computer Incident Advisory Capability, 1994.
- [145] Porras, P. "STAT, A State Transition Analysis Tool for Intrusion Detection." Master thesis, Computer Science Department, University of California, Santa Barbara, CA, 1992.
- [146] Porras, P. and P.G. Neumann. "Emerald: Event monitoring enabling responses to anomalous live disturbances." *National Information Systems Security Conference*, Baltimore, MD, 1997.
- [147] Porras, P. and R.A. Kemmerer. "Penetration State Transition Analysis: A Rule-Based Intrusion Detection Approach." *Proceedings of the Eighth Annual Computer Security Applications Conference*, San Antonio, TX, 1992.
- [148] Portnoy, L., Eleazar Eskin, and Salvatore J. Stolfo. "Intrusion detection with unlabeled data using clustering." *Proceedings of ACM CSS Workshop on Data Mining Applied to Security*, 2001.
- [149] Price, Katherine E. "Host-Based Misuse Detection and Conventional Operating Systems' Audit Data Collection." Master thesis, Purdue University, W. Lafayette, IN, 1997.
- [150] Proctor, P.E. "Practical Intrusion Detection Handbook." Prentice Hall, 2000.
- [151] Puketza, N., K. Zhang, M. Chung, B. Mukherjee, and R.A. Olsson. "A Methodology for Testing Intrusion Detection Systems." *IEEE Transactions on Software Engineering* 22,10, 719-729, 1996.
- [152] Puketza, N., M. Chung, R.A. Olsson, and B. Mukherjee. "A Software Platform for Testing Intrusion Detection Systems" *IEEE Software* 14, no. 5, 43-51, 1997.
- [153] Reavis, J., "Do you have an intrusion detection response plan?" *Network World Fusion*, September 13, 1999.
- [154] Roesch, M. "Snort – lightweight intrusion detection for networks." *Proceedings of Lisa '99*, 1999.
- [155] Samfat, D. and R. Molva, "IDAMN: An Intrusion Detection Architecture for Mobile Networks", *IEEE Journal on Selected Areas in Communications*, 15, 7, 1997.
- [156] SANS Institute Resources, "What is the role of a file integrity checker like Tripwire in intrusion detection?" SANS Institute Resources, *Intrusion Detection FAQ*, 2000.

- [157] Scambray, J.; McClure, S. and J. Broderick, "Network intrusion-detection solutions", *InfoWorld*, May 4, 1998. InfoWorld Corporation. 1998.
- [158] Schneier, B. *Secrets and lies: Digital Security in a Networked World*. John Wiley, New York, NY 2000.
- [159] Sebring, M., E. Shellhouse, M. Hanna and R. Whitehurst. "Expert Systems in Intrusion Detection: A Case Study." *Proceedings of the 11th National Computer Security Conference*, 1988.
- [160] Seleznyov, A., and S. Puuronen. "Anomaly Intrusion Detection Systems: Handling Temporal Relations Between Events." *Proceedings of the Second International Workshop on Recent Advances in Intrusion Detection*, W. Lafayette, IN, 1999.
- [161] Sherif, J.; R. Ayers and T. Dearmond. "Intrusion Detection," OMEGA, March. 2002
- [162] Shieh, S. and V.D. Gligor. "A Pattern-Oriented Intrusion Detection Model and Its Applications." *Proceedings of the 1991 IEEE Symposium on Research in Security and Privacy*, Oakland, CA, 1991.
- [163] Shimomura, T., *Takedown*. "The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw—By the Man Who Did It." New York, *Hyperion*, 1996.
- [164] Sibert, W. Olin. "Auditing in a Distributed System: SunOS MLS Audit Trails." *Proceedings of the Eleventh National Computer Security Conference*, Washington, DC, 1988.
- [165] Simonian, R., "A Neural Network Approach Towards Intrusion Detection." *Proceedings of the Thirteenth National Computer Security Conference*, Washington, DC, 1990.
- [166] Sinclair, C., L. Pierce, S.P. Matzner. "An Application of Machine Learning to Network Intrusion Detection." *15th Annual Computer Security Applications Conference*, 1999.
- [167] Slatalla and J. Quittner, *Masters of Deception: The Gang That Ruled Cyberspace*. Harper, New York, NY. 1996.
- [168] Smaha, S. and S. Snapp. "Method and System for Detecting Intrusion into and Misuse of a Data Processing System." US555742, U.S. Patent Office, September 17, 1996.
- [169] Smaha, S. E. "Haystack: An Intrusion Detection System." *Proceedings Fourth Aerospace, Orlando, Florida*, 1988.
- [170] Snapp, S., J. Brentano, G. Dias, T. Goan, T. Grance, T. Heberlein, C. Ho, K. Levitt, B. Mukherjee, D. Mansur, K. Pon, and S. Smaha. "A System for Distributed Intrusion Detection." *Proceedings of COMPCON Spring '91*, San Francisco, CA, 1991.
- [171] Sobirey, M., B. Richter, and H. Konig. "The Intrusion Detection System AID: Architecture, and Experiences in Automated Audit Analysis." *Proceedings of the IFIPTC6/TC11 International Conference on Communications and Multimedia Security*, Essen, Germany, 1996.
- [172] Spitzner, L. *Know Your Enemy: Revealing the Security Tools, Tactics and Motives of the Blackhat Community*. Addison Wesley Pub. 2001.
- [173] Staniford, S-Chen; S.Cheung; R. Crawford; M. Dilger; J. Frank, J. Hoagland; K. Levitt; C. Wee; R. Yip and D. Zerkle, "GrIDS-- A Graph-Based Intrusion Detection System for Large Networks" *The 19th National Information Systems Security Conference*, Baltimore, MD, 1996.
- [174] Staniford-Chen, S., B. Tung, and D. Schnackenberg. "The common intrusion detection frame-work (CIDF)." In *Proceedings of the Information Survivability Workshop*, 1998.
- [175] Sterling, B., "The Hacker Crackdown." New York, Bantam. 1992.
- [176] Stolfo, S.J., W. Fan, W. Lee, A. Prodromidis, P. Chan. "Cost-based Modeling for Fraud and Intrusion Detection: Results from the JAM Project." *Proceedings of the 2000 DARPA Information Survivability Conference and Exposition*, 2000.
- [177] Stoll, C., "The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage," New York: Pocket Books. 1990.
- [178] Sundaram, A., "An Introduction to Intrusion Detection", *Crossroads: The ACM Student Magazine*, 2, 4, 1996, Hyperlink: acm.org/Crossroads, 1996.
- [179] Tener, W. "AI and 4GL: Automated Detection and Investigation and Detection Tools." *Proceedings of the IFIP Security Conference*, Sydney, Australia, 1988.
- [180] Tener, W. "Discovery: An Expert System in the Commercial Data Security Environment." *Proceedings of the IFIP Security Conference*, Monte Carlo, 1986.
- [181] Teng, H.S., K. Chen and S. C. Lu. "Security Audit Trail Analysis Using Inductively Generated Predictive Rules." *Proc. 11th National Conference on Artificial Intelligence Applications*, 24-29, IEEE Service Center, Piscataway, NJ, 1990.
- [182] Teng, H.S., K. Chen, and S.C.Lu. "Adaptive Real-Time Anomaly Detection Using Inductively Generated Sequential Patterns." *Proceedings of the 1990 IEEE Symposium on Research in Security and Privacy*, Oakland, CA, 1990.

- [183] Ting, Christopher, T.H. Ong, Y.T. Tan, and P.Y. Ng. "Intrusion Detection, Internet Law Enforcement, and Insurance Coverage to Accelerate the Proliferation of Internet Business." *Proceedings of the Second International Workshop on Recent Advances in Intrusion Detection*, W. Lafayette, IN, 1999.
- [184] Toxen, B. "Real World Linux Security: Intrusion Prevention, Detection, and Recovery." Prentice Hall, 2000.
- [185] TRW Defense Systems Group. "Intrusion Detection Expert System Feasibility Study." Final report 46761, 1986.
- [186] Tsudik, G. and R. Summers. "AudES—"An Expert System for Security Auditing." *Proceedings of the AAAI Conference on Innovative Applications in AI*, San Jose, CA, 1990, reprinted in *Computer Security Journal* 6,1, 89-93, 1990.
- [187] Vaccaro, H. S.; and G. E. Liepins, "Detection of anomalous computer session activity," *Proceedings Symposium on Research in Security and Privacy*, Oakland, CA, 1989.
- [188] Valcarce, E.M., G.W. Hoglund, L. Jansen, and L. Baillie. "ESSENSE: An Experiment in Knowledge-Based Security Monitoring and Control." *Proceedings of the Third USENIX Unix Security Symposium*, Baltimore, MD, 1992.
- [189] Vert, G., D.A. Frincke, and J. McConnell. "A Visual Mathematical Model for Intrusion Detection." *Proceedings of Twenty-First National Information System Security Conference*, Crystal City, VA, 1998.
- [190] Warrender, C., S. Forrest, and B. Pearlmutter. "Detecting Intrusions Using System Calls: Alternative Data Models." *Proc. of the IEEE Symposium on Security and Privacy*, 133-145. IEEE Computer Society, 1999.
- [191] Wee, C. "LAFS: A Logging and Auditing File System." *Proceedings of the Eleventh Computer Security Applications Conference*, New Orleans, LA, 1995.
- [192] Wee, C., "Policy-Directed Auditing and Logging." Ph.D. thesis, University of California, Davis, CA, 1996.
- [193] Weiss, W. and A. Baur. "Analysis of Audit and Protocol Data Using Methods from Artificial Intelligence." *Proceedings of the Thirteenth National Computer Security Conference*, Washington, DC, 1990.
- [194] Wetmore, B. "Audit Browsing." Master thesis, University of California, Davis, CA 1993.
- [195] White, G., E.A. Fisch, and U.W. Pooch. "Cooperating Security Managers: A Peer-Based Intrusion Detection System." *IEEE Network* 10,1, 20-23, 1996.
- [196] Winkler, J. "Intrusion and Anomaly Detection: ISOA."
- [197] Winkler, J. "UNIX Prototype for Intrusion and Anomaly Detection in Secure Networks." *Proceedings of the 13th National Computer Security Conference*, October 1990.
- [198] Winkler, J. and W. J. Page, "Intrusion and Anomaly Detection in Trusted Systems," *Proceedings of the Fifth Annual Computer Security Applications Conference*, Tucson, AZ., 1989.
- [199] Wood, M. "Intrusion Detection Exchange Format Requirements." Internet draft, *Internet Engineering Task Force*, 1999.
- [200] Ye, N. "A Markov chain model of temporal behavior for anomaly detection." *Proceedings of the IEEE Systems, Man, and Cybernetics Information Assurance and Security Workshop*, 2000.
- [201] Yip, R. and K. Levitt. "Data Level Inference Detection in Database Systems." *Proceedings of the Eleventh IEEE Computer Security Foundations Workshop*, Rockport, MA, 1998.
- [202] Yuill, K., S.F. Wu, F. Gong, and M-Y. Huang, "Intrusion Detection for an Ongoing Attack." *Proceedings of the Second International Workshop on Recent Advances in Intrusion Detection*, W. Lafayette, IN, 1999.
- [203] Zamboni, D. and E. Spafford. "New Directions for the AAFID Architecture." *Proceedings of the Second International Workshop on Recent Advances in Intrusion Detection*, W. Lafayette, IN, 1999.
- [204] Zamboni, D. "SAINT: A Security Analysis Integration Tool." *Systems Administration, Networking and Security (SANS) Conference*, Washington, DC, 1996.
- [205] Zerkle, D. and K. Levitt. "NetKuang—A Multi-Host Configuration Vulnerability Checker." *Proceedings of the Sixth USENIX Security Symposium*, San Jose, CA, 1996.
- [206] Zirkle, L., "What is host-based intrusion detection?" Virginia Tech CNS. *SANS Institute Resources, Intrusion Detection FAQ*, Hyperlink: ID FAQ, 2000.