Analysis of Intrusion Detection Tools for Wireless Local Area Networks

[1] Jatinder Singh, [2] Dr. Lakhwinder Kaur,[3] Dr. Savita Gupta
[1] Asst. Prof., Department of Computer Engineering. Universal Institute of Engg. & Tech., Lalru-Chandigarh (PB)-India.

[2] Reader, Department of Comp. Engg., UCOE, Punjabi University, Patiala(PB)-India.
[3] Professor, Department of Comp. Engg., UIET, Punjab University, Chd.(PB)-India

Summary
Intrusion-detection systems endeavor at detecting attacks against networks or, in general, against information systems. Undeniably, it is convoluted to provide provably secure network and to maintain them in such a secure state during their lifetime and utilization. Sometimes, legacy or operational constraints do not even allow the definition of a fully secure network. Therefore, intrusion detection systems have the task of monitoring the usage of such systems to detect any apparition of insecure states. They detect attempts and active misuse either by legitimate users of the systems or by external parties to abuse their privileges or exploit security vulnerabilities.[1] This paper covers overview and analysis of Intrusion Detection Systems tools for detecting intrusions in Wireless Local Area Networks (WLAN). Twenty five research and commercial systems are evaluated based on some common parameters. A taxonomy especially designed for intrusion detection systems (IDS) is utilized to compare and evaluate different features and aspects of the products. This paper identifies a number of important design and implementation issues which provide a framework for evaluating or deploying intrusion detection systems.

Key words:
IDS, Wireless, LAN.

1. Introduction

Intrusion detection systems (IDSs) collect and scrutinize the data to recognize computer system and network intrusions and mishandlings. The conventional IDSs have been designed for wired systems and networks to identify intrusions and mishandling. Of late, wireless networks have been concentrated for employing the IDSs constructed. Monitoring and analyzing user and system activities, recognizing patterns of known attacks, identifying abnormal network activity, and detecting policy violations for WLANs are the functions of these wireless IDSs. Wireless IDSs collect all local wireless transmissions and rely either on predefined signatures [3] or on anomalies in the traffic [4] to produce alerts.

Manuscript received July 5, 2009
Manuscript revised July 20, 2009

1.1 Intrusion & Intrusion Detection Systems

Intrusion: Webster's dictionary defines an Intrusion as "The act of thrusting in , or of entering into a place or state without invitation , right or welcome." Or An intrusion is an active sequence of related events that deliberately try to cause harm, such as rendering system unusable, accessing unauthorized information, or manipulating information.

Intrusion detection system (IDS)
An intrusion-detection system (IDS) can be defined as the tools, methods, and resources to help identify accesses, and report unauthorized or unapproved network activity.

OR

- Intrusion detection systems (IDSs) are software designed for detecting; blocking and reporting unauthorized activity in computer networks.

1.2 Types of Intrusion Detection Systems

There are two primary types of IDS: host-based (HIDS) and network-based (NIDS). A HIDS resides on a particular host and looks for indications of attacks on that host. A NIDS resides on a separate system that watches network traffic, looking for indications of attacks that traverse that portion of the network.

1.2.1 Host-Based IDS

HIDS exists as a software process on a system. HIDS examines log entries for specific information. Periodically, the HIDS process looks for new log entries and matches them up to pre-configured rules. If a log entry matches a rule, the HIDS will alarm.

1.2.2 Network-Based IDS

NIDS exists as a software process on a dedicated hardware system. The NIDS places the network interface card on the system into promiscuous mode, i.e. the card passes all traffic on the network to the NIDS software. The traffic is then analyzed according to a set of rules and attack

signatures to determine if it is traffic of interest. If it is, an event is generated.

2. Anomaly vs. Misuse detection

At the heart of intrusion detection lies the ability to distinguish acceptable, normal system behavior from that which is abnormal (possibly indicating unauthorized activities) or actively harmful. Two approaches to this problem can be distinguished, with IDS implementations using some combination of these:

2.1 Anomaly detection attempts to model normal behavior. Any events which violate this model are considered to be suspicious. For example, a normally passive public web server attempting to open connections to a large number of addresses may be indicative of a worm infection.

2.2 Misuse detection attempts to model abnormal behavior, any occurrence of which clearly indicates system abuse. For example, an HTTP request referring to the cmd.exe file may indicate an attack. Anomaly detection suffers from accuracy problems, as building an accurate model (avoiding false negatives) may not fully reflect the complex dynamic nature of computer systems (leading to false positives). This technique has had some success in detecting previously-unknown attack techniques, a major shortcoming in misuse detection. Misuse detection, by virtue of the simpler scope of the objects being modelled, can attain high levels of accuracy. The major difficulty with this approach, however, lies in creating compact models of attacks - models that cover all possible variants of an attack, while avoiding benign patterns. In addition, this approach is vulnerable to novel attacks (attacks dissimilar to all previously known examples) – arguably the most dangerous kind. Due to the complementary nature of these two approaches, many systems attempt to combine both of these techniques. The problem of false positives cause many commercial IDS offerings to focus on misuse detection - leaving anomaly detection to research systems.

3. Network Intrusion Detection System (NIDS)/ Host Intrusion Detection System (HIDS)

3.1 Network Based Intrusion Detection

Network-based intrusion detection systems use raw network packets as the data source. A network-based IDS typically utilizes a network adapter running in promiscuous mode to monitor and analyze all traffic in real-time as it travels across the network. Its attack recognition module uses four common techniques to recognize an attack signature:

- Pattern, expression or byte code matching,
- Frequency or threshold crossing
- Correlation of lesser events
- Statistical anomaly detection

Once an attack has been detected, the IDS' response module provides a variety of options to notify, alert and take action in response to the attack. These responses vary by product, but usually involve administrator notification, connection termination and/or session recording for forensic analysis and evidence collection.

3.2 Host Based Intrusion Detection

Host-based intrusion detection started in the early 1980s before networks were as prevalent, complex and interconnected as they are today. In this simpler environment, it was common practice to review audit logs for suspicious activity. Intrusions were sufficiently rare that after the-fact analysis proved adequate to prevent future attacks.

Today's host-based intrusion detection systems remain a powerful tool for understanding previous attacks and determining proper methods to defeat their future application. Host-based IDS still use audit logs, but they are much more automated, having evolved sophisticated and responsive detection techniques.

4. Methodology

In order to evaluate the divergent products on the souk, we examined publicly available research papers, reports, product documentation, published conference material (proceedings) and other material available for public review. As this paper is an analysis of design specifications rather than a test of execution.

5. Research Parameters

For detailed analysis of Research /Industrial/Commercially available Intrusion Detection Systems , we have chosen some parameters. Definition of those parameters is as follows:

1. Granularity of Data Processing: It refers to the response time of an Intrusion Detection System depends partly on the granularity of data processing. The

unprocessed data collected for the processing can be processed ad infinitum or in consignments, at some regular interval. The most of the system are working on Real-time i.e. ad infinitum and few systems are working on manual by grouping batches or consignments.

2. Audit source location: It refers to the location of the Intrusion detection system .The audit source location discriminates intrusion-detection systems based on the kind of input information they analyze. This input information can be audit trails (such as system logs) on a host, network packets, application logs, or intrusion-detection alerts generated by other intrusion-detection systems. The source of audit data can be either network- or host-based. Network-based data are usually read directly off some multicast network (Ethernet). Host-based data (security logs) are collected from hosts distributed all over the network and can include operating system kernel logs, application program logs and network equipment logs or other host-based security logs.

3. Management Console: This parameter refers to management console i.e. the user interface that the client component of network management software provides. It is the user interface and "control room" view of the network. A terminal or workstation used to monitor and control a network. There are the different values of this parameter i.e. Excellent, Accustomed i.e. comfortable user interface and the Intricate that is complicated for the user to view the network.

Sr.No.	Intrusion Detection System	Vendor
1	Snort	Snort Corporation
2	Dragon	Enterasys Corporation
3	Cisco Secure IDS	Cisco system, Inc.
4	Emerald	SRI International
5	Net Ranger	Cisco Systems, Inc.
6	Tripwire	Purdue University
7	Intruder Alert	Axent Technologies, Inc.
8	Netstat	University of California at Santa Barbara
9	CMDS	Science Application International Corporation (SAIC)
10	Entrax	Centrax Corporation
11	Bro	Centrax Corporation
12	Stake Out I.D	Harris Communications, Inc
13	SecureNet PRO	MimeStar, Inc.
14	Kane Security Monitor	Security Dynamics (formerly Intrusion Detection, Inc.)
15	NetProwler	Axent Corporation
16	Session Wall-3	AbirNet
17	Network Flight Recorder	Network Flight Recorder, Inc.
18	INTOUCH INSA	Touch Technologies, Inc
19	RealSecure	Internet Security Systems (ISS)
20	CyberCop	Network Associates, Inc.
21	ID-Trak	Internet Tools, Inc
22	NIDES	SRI International
23	T-Sight	EnGarde Systems, Inc.
24	Shadow	Network Research Group (Lawrence Berkeley Lab)
25	SecureCom Suite	ODS Networks

4. Behavior on Attack: It describes the response of the intrusion-detection system to attacks. On the basis of their response to Intrusion, IDS can be either Active or Passive. An active IDS actively reacts to the attack by taking either corrective (closing holes) or pro-active (logging out possible attackers, closing down services) actions, then the intrusion-detection system is said to be active. And when the intrusion-detection system merely generates alarms (such as paging), it is said to be passive. Most of the system analyzed are actively detects the intruders few are passive and few are detecting intruders using both actively and passively behavior.

5. Reporting Capability: This parameter is related to how quick an IDS reports about the attack to the network administrator. In today's scenario, real time IDS is preferred as it reports about attack as soon as it occurs. We have classified it as two values i.e. High and Medium.

6. Interoperability: The interoperability is the measures of the intrusion detection system's ability to cooperate with other similar systems. Interoperability can be of interest at various levels in the architecture serving many different purposes such as:

- Exchange of audit data records
- Exchange of security policies
- Exchange of misuse patterns or statistical information about user activities.

6. Systems analyzed

A total of 25 Research and Commercial Intrusion Detection systems Tools were analyzed in this survey.

7. Results

As already mentioned, a total of 25 different intrusion detection systems were analyzed in this survey. The results are categorized using the criteria defined by the different taxonomic criteria. For each category listed, it is the aim to give a comparative view of the conformance of the

7.1 Functional Aspects of Tools

1. Granularity of data processing
Almost all of the vendors allow intrusions to be detected in real-time. A relevant question in this context is how to interpret "real-time". The time that elapses between the time an attack is initiated and until the system is penetrated varies depending on the nature of the attack. Assuming that automated tools are used for the attack, the time to a complete collapse of system security may be in the order of milliseconds. Therefore, in some cases, the attack may be completed before it is detected and reported to the proper authority. Another issue is the real-time characteristics of host-based intrusion detection systems. In this case, audit logs are collected in batches before they are processed or analyzed, with an even longer delay as a result.

2. Audit Source Location
A majority of the analyzed systems are network oriented in terms of source of audit data. Only six systems are purely host-based and four systems support both host- and network-based audit data. As previously mentioned in the section on comparison criteria the increasing use of switched network technologies and encryption jeopardizes the future of network-based systems. Still, most systems of today rely upon network audit data. Some vendors claim that switched networks can easily be analyzed using dedicated management ports on the switches. This may be true if the network is moderately loaded but it is unrealistic on medium or heavily loaded networks. An innovative solution is provided by ODS Networks Inc. They incorporate ID (provided by ISS Inc.) into their product line of switches, thus eliminating the restrictions posed by switching technology. Although solutions exist to address the problem of switching, network encryption is a greater challenge. Confidentiality requirements prevent IDS from interpreting the semantics of the data streams. From a confidentiality requirement standpoint, an IDS is just like any other unauthorized adversary.

3. Management console:-The most of the system analyzed are provide console based user interface few are also provide the graphical user interface to view the activities. Snort provides good management Console**.** It provides this feature with the help of ACID plug-in module. Plug-in are very important feature of Snort IDS. These are programs that are written to conform to Snort's plug-in API. These programs used to be part of the core Snort code, but were separated out to make modifications to the core source code more reliable and easier to accomplish. ACID stands for The **Analysis Console for Intrusion Databases**. It provides logging analysis for Snort. Requires PHP, Apache, and the Snort database plug-in. Since this information is usually sensitive, it is strongly recommended that we encrypt this information by using mod_ssl with Apache or Apache-SSL. Dragon provides an excellent management console. This feature is implemented in **'Dragon Enterprise Management Server' component.** This component is made up of a number of highly integrated technologies. Web based and centralized, Policy Management tools offer enterprise-wide management of small and large-scale Dragon deployments. Dragon Policy Manager provides centralized management of the Dragon Network and Host Sensors, while Alarm tool offers centralized alarm and notification management. **Cisco** provides management console but it's not so good in comparison to that of Snort & Dragon. It is responsible for the communication between the server and the agents. Communication between agents and the server take place at intervals set in the console. The communication port for the console and the agent must be the same for them to communicate**.** It also contains the list indicating state of each agent.

4. Behavior on Attack
Passive Passive responses. Passive response means that an intrusion is brought to the attention of the SSO. Mechanisms for passive response may be sending e-mails, paging or displaying alert messages. Many systems provide some support for passive response mechanisms.
Active response. All but three systems (Stake Out, Kane Security Monitor and TSight) support active response without human interaction. For network-based systems, active response include actions like terminating transport level sessions, which most active response systems claim they support. Some systems, such as SecureNet Pro, even allow the SSO to hijack a TCP session. Host-based ID systems have the advantage that they can also control hostile processes on the host on which they reside. Most host-based systems analyzed claim to support termination of processes. Kane Security Monitor does not have this feature. Entrax offers only the possibility to log out a user, disable a users account or shut down the entire computer, which can be seen as a drastic way of terminating processes. Emergency shutdown of the entire host can be

useful when the system contains information whose confidentiality is more important than its availability. Systems contaminated by computer viruses may also benefit from being shut down to prevent further contamination. A security breach in the IDS itself may be exploited to attack the target system.

The most important system like Snort can be used for Active as well as passive monitoring of the network. Passive monitoring is simply the ability to listen to network traffic and log it. Cisco can behave actively or passively on the choice of the user. It includes a feature called Policy Management, which allows the user to decide how to react on the occurrence of an attack. Reactions towards attack can be as follows: -

- **Ignore:** Attack is ignored.
- **Log:** Attack is logged in the database.
- **Prevent: A**ttack is logged and the specific illegal operation is prevented from taking place.
- **Terminate Process:** Attack is logged and the process that is performing the attack is terminated.

5. Reporting capabilities

The detection capabilities between products vary quite extensively. In general, a network- based IDS has greater capabilities owing to its ability to capture and analyze packet at the underlying network. Host-based ID systems are limited to audit-logs provided by the operating system or application logs. Due to the large number of different intrusions recognized, this paper present only an overview of the types of attacks each product can detect. Some of the products, such as RealSecure and Intruder Alert, include up to 200 different known intrusion signatures out of the box. Table 5 shows the detection capabilities mapped onto a simple protocol stack. Cisco performs real time attack detection using Intrusion Detection System Module (IDSM)**.** The IDSM performs network sensing in real-time. It monitors network packets through packet capture and analysis. Dragon provides real time attack reporting. Dragon Host Sensor component monitors key system logs for evidence of tampering. Dragon Enterprise Management Server provides complete monitoring and control. To support real-time monitoring it allows events to be viewed as they occur, providing an understanding what may have changed, or what is happening at that moment within the security system Snort is a real time IDS. Snort provides attack alert messages to be sent via e-mail to notify a system administrator in real time. This way no one has to monitor the Snort output all day and night.

Sr.No.	Intrusion Detection System	Granularity of data processing	Audit Source Location	Management Console	Behavior on Attack	Reporting Capability	Interoperability
1	Snort	Realtime	NIDS	Accustomed	Passive/Active	High	Medium
2	Dragon	Realtime	NIDS/HIDS	Excellent		High	High
3	Cisco Secure IDS	Realtime	NIDS	Intricate	Passive/Active	High	Medium
4	Emerald	Realtime	NIDS	Accustomed	active	Medium	
5	Net Ranger	Realtime	NIDS	Intricate	Active	High	Medium
6	Tripwire		HIDS	Intricate			
7	Intruder Alert	Realtime	NIDS/HIDS	Accustomed	Active	High	Medium
8	Netstat	Realtime	NIDS	Intricate	Active		
9	CMDS	Realtime	HIDS	Accustomed	Active	Medium	Low
10	Entrax	Realtime	HIDS	Accustomed	Active	Medium	
11	Bro	Realtime	NIDS	Accustomed	Active		
12	Stake Out I.D	Realtime	NIDS	Excellent	Passive	High	Low
13	SecureNet PRO	Realtime	NIDS	Excellent	Active	High	Low
14	Kane Security Monitor	Realtime	HIDS	Accustomed	Passive	Medium	Low
15	NetProwler	manual	HIDS	Intricate	Active		
16	Session Wall-3	Realtime	NIDS	Excellent	Active	High	Medium
17	Network FlightRecorder	Realtime	NIDS	Accustomed	Active	High	Low
18	INTOUCHINSA	Realtime	NIDS	Excellent	Active	Medium	Low
19	RealSecure	Realtime	NIDS/HIDS	Excellent	Active	High	Medium
20	CyberCop	Real time	NIDS/HIDS	Accustomed	Active	High	Medium
21	ID-Trak	Real-time	NIDS	Accustomed	Active	Medium	Low
22	NIDES	Real time	HIDS	Intricate	Active	High	Low
23	T-Sight	manual	NIDS	Intricate	Passive	-	None
24	Shadow	manual	NIDS	Intricate	Active		
25	SecureCom Suite	Real time	NIDS	Excellent	Active	High	Medium

6. Interoperability

Interoperability for IDS can be achieved in a number of different areas. Four important areas are the Exchange of audit data records, Exchange of security policies, Exchange of misuse patterns or statistical information about user activities and Exchange of alarm reports, event notifications and response mechanisms

Exchange of audit data records. Having a well defined data format for the audit records would let several IDS analyze the same data. This would be of importance if a decision is made to change the IDS or to have a second IDS analyze the same set of data. Network-based IDS listen to the network-level data stream, and thus collection of data is not always necessary. However, for host-based systems, interoperability would be beneficial. To some extent, interoperability exists in the products of today. For example, many IDS can make use of operating system audit logs, which may have a well defined format. In the Exchange of security policies we are Having a series of protection mechanisms to protect a network increases the depth of protection. In this case, the IDS will be able to detect security violations within the network as well as detect external violations not detected by the firewall. Although this scenario would be beneficial, it can cause a management problem as the security policy must be distributed to both the firewall and the IDS. As of today, the security policy is usually defined in a proprietary format for each and every component and cannot easily be exported or shared by other components. A firewall cannot use the policy of an IDS or vice versa. This means that it may be necessary to maintain several sets of policies, although their semantics are the same. As far as we could find, none of the IDS vendors address this problem. The Exchange of misuse patterns or statistical information about user activities. This is perhaps one of the most controversial interoperability aspects. Vendors providing a large set of misuse patterns of known intrusions have a competitive edge, hopefully resulting in increased sales. Although a standardized way of representing, storing and distributing misuse patterns using some form of vulnerability database[5] would benefit the users of the IDS, the vendors will probably not provide this feature in the near future. No IDS analyzed here has this feature. The last exchange i.e. the Exchange of alarm reports, event notifications and response mechanisms.

Sr.No.	Intrusion Detection System	SMTP	Paging	SNMP	OPSEC (Incl. FW-1)	Raptor (FW from Axent)	Pix (FW from Cisco)	Cisco Routers	Lucent FW Security Mgmt. Server
1	Snort	*	*	*					
2	Dragon	*		*					
3	Cisco Secure IDS	*	*	*			*	*	
4	Emerald	*		*					
5	Net Ranger	*	*	*				*	
6	Tripwire								
7	Intruder Alert	*	*	*	*	*		*	
8	Netstat	*							
9	CMDS								
10	Entrax	*	*	*					
11	Bro								
12	Stake Out I.D	*	*	*					
13	SecureNet PRO	*							
14	Kane Security Monitor	*	*	*					
15	NetProwler	*							
16	Session Wall-3	*	*	*	*			*	
17	NetworkFlight Recorder	*	*						
18	INTOUCH INSA								
19	RealSecure	*		*	*				*
20	CyberCop	*	*	*			*		
21	ID-Trak	*	*	*					
22	NIDES								
23	T-Sight								
24	Shadow								
25	SecureCom Suite	*		*	*				*

Detection Method: It is the capability of the IDS to detect various types of attacks. This depends on the number of signatures defined in the knowledge base of the IDS.

Sr. No.	Product	Rule Based	Anomaly Based
1	Snort	*	
2	Dragon	*	*
3	Cisco Secure	*	
4	Emerald	*	
5	Net Ranger	*	
6	Tripwire	*	
7	Intruder Alert	*	
8	Netstat	*	*
9	CMDS	*	*
10	Entrax	*	
11	Bro	*	
12	Stake Out I.D	*	*
13	SecureNet	*	
14	Kane Security	*	*
15	NetProwler	*	
16	Session Wall-3	*	
17	Network Flight	*	
18	INTOUCH I	*	*
19	RealSecure	*	
20	CyberCop	*	
21	ID-Trak	*	
22	NIDES	*	*
23	T-Sight	*	
24	Shadow	*	
25	SecureCom Suite	*	

Rule based detection. The system detects the violation of a policy. A policy is described by a set of rules. This policy can be specified either in a default permit or in a default deny fashion. Using a default permit stance, the SSO specifies some kind of signature that describes illicit behavior. Finding these signatures can be as simple as performing pattern recognition or can be more advanced, e.g using some form of state machine. In a default deny stance, the SSO specifies the normal operation of the system, and deviations from the set norm are viewed as an attempted intrusion by the detection function. When evaluating intrusion detection systems, one should not underestimate the value of the mechanism used for providing rule based detection. Some systems, for example RealSecure and Cisco's NetRanger, use a simple mechanism similar to regular expressions to find strings or patterns that violate some policy or rule. Although regular expressions or other pattern matching mechanisms can be powerful, they do not allow themselves to represent state information. Using some form of state-machine or programming language, arbitrary complex programming constructs may be used by the detection mechanism.

Anomaly based detection. The system reacts to anomalous behavior, as defined by some history of the monitored target. In this definition, we also include the systems ability to automatically learn from the past. Anomaly based detection often uses some form of statistical or artificial intelligence (AI) engine. For example, PolyCenter, Stake Out I.D. and KSM use AI for that purpose. CMDS and NIDES find anomalies by calculating statistical deviations. Network Flight Recorder's flexible programming language should make it possible to implement customized detection methods such as anomaly based detection.

7.2 Architectural aspects

System organization

Virtually every system can operate in a distributed environment. Only INTOUCH INSA and T-Sight are limited to a single host or network segment. Intruder Alert (IA) is partly distributed. While the host-based IA can operate distributed under centralized control, its network-based system (NetProwler) cannot.

System and network infrastructure requirements

Operating Systems. Despite the market trend to migrate applications to Windows NT, a surprisingly number of ID systems operate in various UNIX environments. Table below contains a summary of the operating system requirements for the manager and agent side for each IDS. It is worth mentioning that Axent supports an impressive number of operating systems for Intruder Alert.

Protocol. As expected, TCP/IP is the dominating protocol suite supported. Table 8 gives a summary of network technologies supported by each product.

7.3 Operational aspects

Performance aspects

Communication overhead. Few of the analyzed systems specify the communication overhead induced by deploying intrusion detection. For network-based intrusion detection, the overhead is caused by the distribution of audit data and the communication

between the various subsystems of the IDS. For RealSecure, ISS reported a network load overhead of 5-10%

Computational overhead. Computational overhead applies mainly to host-based IDS. While network-based ID systems usually run on a dedicated system, host-based IDS execute and collect audit data on the target they monitor. The performance penalty depends greatly on such parameters as granularity of data processing, size and

growth rate of system logs, size and complexity of the ID rulebase etc.

Sr.No.	Intrusion Detection System	Operating System Support	Protocol
1	Snort	MS Windows, LINUX	TCP/IP
2	Dragon	MS Windows, LINUX, Solaris	TCP/IP
3	Cisco Secure IDS	MS Windows, UNIX	TCP/IP
4	Emerald	MS Windows, UNIX	TCP/IP
5	Net Ranger	Solaris	TCP/IP
6	Tripwire	UNIX	
7	Intruder Alert	Solaris, Sun OS	TCP/IP,IPX/SPX
8	Netstat	UNIX	
9	CMDS	Solaris, NT	_
10	Entrax	NT, UNIX	_
11	Bro	UNIX	
12	Stake Out I.D	Solaris	TCP/IP
13	Secure Net PRO	Solaris , LINUX	TCP/IP
14	Kane Security Monitor	NT	TCP/IP
15	Net Prowler	MS Windows, UNIX	
16	Session Wall-3	NT, W95/98	TCP/IP
17	NetworkFlight Recorder	Red Hat LINUX, Solaris	TCP/IP
18	INTOUCH INSA	Not Applicable	TCP/IP
19	Real Secure	NT, Solaris	TCP/IP
20	Cyber Cop	NT, Solaris	TCP/IP
21	ID-Trak	NT	TCP/IP
22	NIDES	Sun OS	TCP/IP
23	T-Sight	Not Applicable	TCP/IP
24	Shadow	UNIX	
25	SecureCom Suite	NT, Solaris	TCP/IP

8. Conclusion

In recent years, there has been a dramatic increase in the use of security services such as firewalls. A common belief is that, once a firewall is installed, all security problems are solved. Of course, this is not the case, in contrast to what certain market forces lead us to believe. The same enthusiasm can be found among advocates of intrusion detection systems. However, it is important to understand that intrusion detection systems are not a substitute for other security services such as firewalls, authentication servers etc. They should be regarded as a complement to other security services that further extend the level of protection of the target systems, resources or information. IDS began as a technology for analyzing host-based audit data. In recent years, network-based systems have appeared and extended the capabilities of intrusion detection systems. This survey shows that the majority of the commercial ID systems are network-based systems. In fact, nine of 25 are network-based whereas only five are purely host-based. However, the increasing use of encryption in network infrastructures such as IPSEC seriously limits the IDS ability to access network-based audit data. This limitation may mandate a second shift towards analysis of higher layer protocols for the purpose of intrusion detection. Further, the need for efficient deployment of intrusion detection for security services such as firewalls, authentication services, directory services etc. The security of current commercial ID systems is questionable. Although stegnography and cryptography techniques are used to protect communication links between different components, it is unclear how the information contained in the IDS is protected as a whole. The modularity of current commercial systems leaves much to be desired. Most often, there are no clear boundaries between raw input event collection, detection and response functions. This seriously limits the versatility of the IDS as it does not allow an ID capability to be built using components from different vendors. One of the best examples of this is databases containing known intrusions. Each vendor provides his own proprietary database which cannot be used by other products. In fact, the proprietary databases create a competitive edge toward other vendors. Therefore, it is not likely that an initiative leading to interoperability between intrusion databases would come from a major vendor. The research community and small vendors trying to break the market dominance are more likely to take on such a task.

In the information age of today, the boundaries between software applications and network technologies are fading away. Traditional software vendors are providing applications and services tightly coupled with network infrastructures. A good example of this is IP telephony. At the same time, traditional network element providers are seeking to broaden their portfolio by delivering software packages to assist their traditional range of products. As a result, both parties fall into the pitfalls of each other's traditional domains. It appears that the commercial intrusion detection systems of today are an example of this. An intrusion detection system is an advanced piece of software requiring great software engineering and programming skills to design and create. On the other hand, an IDS is also a high performance network component with extremely high availability and dependability requirements. As most office PC users are painfully aware, availability and dependability are not part of the vocabulary of software vendors. It is the author's belief that most ID systems originate from traditional software vendors rather that from network infrastructure vendors. Most of today's IDS are not yet mature enough for large scale, enterprise wide deployment.

References

[1] Herve Debar, "An Introduction to Intrusion-Detection Systems" IBM Research, Zurich Research Laboratory.

[2] "Cisco Secure Intrusion Detection System Director for UNIX Configuration and Operations Guide Version 2.2.2" ,http://www.cisco-ids.org

[3] "Cisco Secure Intrusion Detection System Director for UNIX Configuration and Operations Guide Version 2.2.2" ,http://www.cisco-ids.org

[4] "Snort-The de-facto standard for intrusion detection-prevention", http://www.snort.org.

[5] Carter, Earl. 'Cisco Secure Intrusion Detection System' Indianapolis, IN: Cisco Press, 2001.

[6] Hakan Albag, "Network & Agent Based Intrusion Detection Systems",

[7] Hakan Albag, "Network & Agent Based Intrusion Detection Systems",

[8] Herve Debar , "An Introduction to Intrusion-Detection Systems" IBM Research, Zurich Research Laboratory.

[9] Herve Debar, "An Introduction to Intrusion-Detection Systems" IBM Research, Zurich Research Laboratory.

[10] http:// www.cert.org

[11] http://www.cisco.com/security/

[12] http://www.enterasys.com/products/ids, "DRAGON 6.0 INTRUSION DETECTION SYSTEM-Data Sheet"

[13] http://www.enterasys.com/products/ids, "Dragon® 7 Network Intrusion Detection and Prevention".

[14] http://www.enterasys.com> Home > Products > Advanced Security Applications > Intrusion Detection/Prevention

[15] http://www.enterasys.com> Home > Products > Advanced Security Applications > Intrusion Detection/Prevention

[16] http://www.scala.com/support

[17] http://www.snort.org

[18] Jay Beale,James C. Foster, "Snort 2.0 Intrusion detection", PUBLISHED BY Syngress Publishing Inc, http://www.syngress.com/solutions

[19] Jay Beale,James C. Foster, "Snort 2.0 Intrusion detection", PUBLISHED BY Syngress Publishing Inc, http://www.syngress.com/solutions

[20] Jones Anita K, Sielken Robert S.: Computer System Intrusion Detection: A Survey. University of Virginia, USA 19–20

[21] Jones Anita K, Sielken Robert S.: Computer System Intrusion Detection: A Survey. University of Virginia, USA 19–20

[22] Jungwon Kim & Peter J. Bentley§ " Immune System Approaches to Intrusion Detection - A Review" www.cs.nott.ac.uk/~uxa/papers/04icaris_ids_review.pdf

[23] K. Ilgun, 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, March 1995.

[24] Krügel Christopher, Toth Thomas: A Survey on Intrusion Detection Systems. TU Vienna , Austria (2000) 7, 22–33

[25] Krügel Christopher, Toth Thomas: A Survey on Intrusion Detection Systems. TU Vienna , Austria (2000) 7, 22–33

[26] L. Zhou and Z. J. Haas. Securing ah hoc networks. IEEE Network, 13(6):24{30, Nov/Dec 1999.

[27] Madge, (2005). Wireless intrusion detection systems (ids) evolve to 3rd generation proactiveprotection systems. Retrieved Apr. 06, 2006, from http://www.telecomweb.com/readingroom/Wi

[28] Jonathan P. Ellch Civilian, Federal Cyber Corps B.S., Purdue University, 2004 "FINGERPRINTING 802.11 DEVICES"ieeexplore.ieee.org/iel5/10599/33505/01592979 .pdf?arnumber=1592979

[29] reless_Intrusion_Detection.pdf

[30] Martin Roesch, "SNORT-Lightweight intrusion detection for networks", Proceedings of LISA '99: 13th Systems Administration Conference Seattle, Washington, USA, November 7–12, 1999.

[31] Mike Chapple, "Snort -- The poor man's intrusion-detection system", http://searchsecurity.techtarget.com.

[32] P. G. Neumann and P. A. Porras, "Experience with EMERALD to date," in Proc. Workshop Intrusion Detection Network Monitoring, Santa Clara, CA, Apr. 1999, pp. 73–80

[33] pcmag.com-encyclopedia

[34] Phillip A. Porras and Alfonso Valdes. "Live traffic analysis of TCP/IP Gateways". In Proceedings of the 1998 ISOC Symposium on Network and Distributed System Security (NDSS'98), San Diego, CA, March 1998. Internet Society.

[35] Ralf Spenneberg, "Super Sniffer", http://www.linux-magazine.com, July-2003.

[36] Ricky M. Magalhaes, Host-Based IDS vs Network-Based IDS (Part 2 -Comparative Analysis), Jul 17, 2003

[37] Rupinder Gill, Jason Smith and Andrew Clark "Specification-Based Intrusion Detection in WLANs "Information Security Institute, Queensland University of Technology GPO Box 2434, Brisbane, 4001, QLD, Australia. doi.ieeecomputersociety.org/10.1109/ACSAC.2006.48

[38] S. Kumar and E. H. Spa_ord. A software architecture to support misuse intrusion detection. In Proceedings of the 18th National Information Security Conference, pages 194{204, 1995.
[39] TU Munich, Dep. of Computer Science, Istanbul Tech. Uni., Deptt. of Comp. Engineering.
[40] TU Munich, Dep. of Computer Science, Istanbul Tech. Uni., Deptt. of Comp. Engineering.
[41] Vaibhav Gowadia,Csilla Farkas,Marco Valtorta, "PAID: A Probabilistic Agent based Intrusion detection system",Information Security Laboratory,University of south carolina,Columbia
[42] Vaibhav Gowadia,Csilla Farkas,Marco Valtorta, "PAID: A Probabilistic Agent based Intrusion detection system",Information Security Laboratory,University of south carolina,Columbia
[43] W. Lee and S. J. Stolfo. Data mining approaches for intrusion detection. In Proceedings of the 7th USENIX Security Symposium, San Antonio, TX, January 1998.
[44] W. Lee, S. J. Stolfo Data Mining Approaches for Intrusion Detection
[45] W. Stallings, Network and Inter-Network Security Principles and Practice. Englewood Cliffs, NJ: Prentice-Hall, 1995.
[46] www.c-com.com.tw/support/c-com-support-glossary.htm
[47] www.c-com.com.tw/support/c-com-support-glossary.htm
[48] www.ez-access.com/glossary.html
[49] www.ez-access.com/glossary.html
[50] www.mma.nrao.edu/development/computing /docs /joint/draft /Glossary.htm
[51] www.mma.nrao.edu/development/computing/docs/joint/draft/Glossary.htm