Introduction

1. Although intrusion detection technology is immature and should not be considered as a complete defense, but at the same time it can play a significant role in overall security architecture. If an organization chooses to deploy an IDS, a range of commercial and public domain products are available that offer varying deployment costs and potential to be effective. Because any deployment will incur ongoing operation and maintenance costs, the organization should consider the full IDS life cycle before making its choice. When an IDS is properly deployed, it can provide warnings indicating that a system is under attack, even if the system is not vulnerable to the specific attack. These warnings can help users alter their installation’s defensive posture to increase resistance to attack. In addition, an IDS can serve to confirm secure configuration and operation of other security mechanisms such as firewalls. Within its limitations, it is useful as one portion of a defensive posture, but should not be relied upon as a sole means of protection. As e-commerce sites become attractive targets and the emphasis turns from break-ins to denials of service, the situation will likely worsen.

Fig1: Typical locations for an intrusion detection system
Many early attackers simply wanted to prove that they could break into systems; increasingly nowadays, the trend is toward intrusions motivated by financial, political, and military objectives. In the 1980s, most intruders were experts, with high levels of expertise and individually developed methods for breaking into systems. They rarely used automated tools and exploit scripts. Today, anyone can attack Internet sites using readily available intrusion tools and exploit scripts that capitalize on widely known vulnerabilities. Today, damaging intrusions can occur in a matter of seconds. Intruders hide their presence by installing modified versions of system monitoring and administration commands and by erasing their tracks in audit and log files. In the 1980s and early 1990s denial-of-service attacks were infrequent and not considered serious. Today, successful denial-of-service attacks can put e-commerce based organizations such as online stockbrokers and retail sites out of business. Successful IDSs can recognize both intrusions and denial-of-service activities and invoke countermeasures against them in real time. To realize this potential, we’ll need more accurate detection and reduced false-alarm rates.

Perspectives on Intrusion: Victims and Attackers

2. Attacks can involve numerous attackers targeting many victims. Defining what constitutes an attack is difficult because multiple perspectives are involved. The attacker viewpoint is typically characterized by intent and risk of exposure. From a victim’s perspective, intrusions are characterized by their manifestations, which might or might not include damage. Some attacks produce no manifestations and some apparent manifestations are caused by system or network malfunctions. Some attacks involve the (involuntary) participation of additional machines, usually victims of earlier attacks. For an intrusion to occur there must be both an overt act by an attacker and a manifestation, observable by the intended victim, that results from that act.

Dimensions of Intrusion Detection

3. We can characterize IDSs in a variety of ways. Here, we choose the system structure, sensed phenomenology, and detection approach. Figure 2 illustrates system structure and sensed phenomenology. The figure shows a small enterprise configured with firewalls to isolate its Web server. Computers configured as network sensors extract suspicious packets from the three main network segments and forward them to a network-specific analysis station. The Web server and workstations run software to monitor suspicious interactions with the operating system and report them to a host-specific analysis station. In addition, the Web server looks for abuses such as CGI-bin exploits that are specific to HTTP servers. The analyzers report to a management console that serves as the IDS’s user interface. The management console alerts the enterprise administration who might, in turn, report intrusions to incident- incident-
response organizations such as the CERT Coordination Center. More elaborate configurations are possible. An analyzer might use inputs from any or all sensed phenomenologies in deciding whether an attack has taken place. Analyzer outputs can also serve as sensed data for other analyzers.

**Fig 2**: Illustrates system structure and sensed phenomenology

**Intrusion Detection Approaches**

4. In classical signal-detection approaches, both the signal and the noise distributions are known, and a decision process must determine whether a given observation belongs to the signal-plus noise distribution or to the noise distribution. Classical signal detectors use knowledge of both distributions in making a decision, but intrusion detectors typically base their decisions either on signal (signature-based detectors) or noise (anomaly-based detectors) characterizations. Each approach has strengths and weaknesses. Both suffer from the difficulty of characterizing the distributions. For signature-based IDS to detect attacks, it must possess an attack description that can be matched to sensed attack manifestations. This can be as simple as a specific pattern that matches a portion of a network packet or as complex as a state machine or neural network description that maps multiple sensor outputs to
abstract attack representation. If an appropriate abstraction can be found, signature-based systems can identify previously unseen attacks that are abstractly equivalent to known patterns. They are inherently unable to detect truly novel attacks and suffer from false alarms when signatures match both intrusive and nonintrusive sensor outputs. Signatures can be developed in a variety of ways, from hand translation of attack manifestations to automatic training or learning using labeled sensor data. Because a given signature is associated with a known attack abstraction, it is relatively easy for a signature-based detector to assign names (such as Smurf or Ping-of-Death) to attacks.

Anomaly-based detectors equate “unusual” or “abnormal” with intrusions. Given a complete characterization of the noise distribution, an anomaly-based detector recognizes as an intrusion any observation that does not appear to be noise alone. The primary strength of anomaly detection is its ability to recognize novel attacks. Its drawbacks include the necessity of training the system on noise with the attendant difficulties of tracking natural changes in the noise distribution.

5. Changes can cause false alarms, while intrusive activities that appear to be normal can cause missed detections. Anomaly-based systems have difficulty classifying or naming attacks. We can also classify IDSs based on the phenomenology that they sense. Network-based systems look at packets on a network segment, typically one serving an enterprise or a major portion of one. While network-based systems can simultaneously monitor numerous hosts, they can suffer from performance problems, especially with increasing network speeds. Many network-based systems make simplifying assumptions about such network pathologies as packet fragmentation and can suffer from resource exhaustion problems when they must maintain attack-state information for many attacked hosts over a long period of time.

6. In spite of these deficiencies, they are popular because they are easy to deploy and manage as standalone components and they have little or no impact on the protected system’s performance. Host-based systems operate on the protected host, inspecting audit or log data to detect intrusive activity. A variety of log and audit functions can serve to drive ID algorithms; these can be supplemented by sensors that monitor the interaction of applications with the host operating system. Host-based systems can monitor specific applications in ways that would be difficult or impossible in a network-based system. They can also detect intrusive activities that do not create externally observable behavior. Because they consume resources on the protected host, they can affect performance substantially. Successful intrusions that gain high levels of privilege might be able to disable host-based IDSs and remove traces of their operation. Installing and effectively using IDSs on networks and hosts requires a broad understanding of computer security.

**Preparation**
7. Before an organization invests in security technologies, it must understand which of its assets require protection and determine the real and perceived threats against those assets. We can characterize threats by the likely type of attack and attacker capabilities (that is, resources and goals) and the organization’s tolerance for loss of, damage to, or disclosure of protected assets. Attacker motives can be arbitrary (curiosity or vandalism) or targeted to meet a specific objective such as revenge or gaining a competitive advantage. Motives can make some forms of attack more likely than others. Gaining a competitive advantage might require compromising specific information such as a marketing plan. Each form of attack requires diverse detection strategies. For example, information retrieval is likely to occur during a stealthy attack, while information corruption might require speed. Determining whether the potential attacker is inside or outside the organization’s infrastructure affects the type and placement of an IDS. Often, the most significant obstacle to an information security improvement initiative is lack of management support. Surveys conducted by security trade magazines cited lack of management support as one of the principle barriers to effective information security. Security only becomes important when it impinges on the organization’s high-priority interests and reputation. Deploying and operating an IDS requires significant management support.

Defense in Depth

8. ID is only one aspect of a layered defensive posture or “defense in depth.” Defense in depth begins with the establishment of appropriate and effective security policies. Effective policies help ensure that threats to critical assets are understood, managers and users are adequately trained, and actions to be taken when an intrusion is identified are defined. A good security policy puts ID in its proper perspective and context. Whenever possible, the policy should reflect the mission of the organization that promulgates it. Therefore, it should codify the rules governing enterprise operations as they are reflected in its information infrastructure and should explicitly exclude activities or operations not needed to support the enterprise’s mission. A mission-oriented security policy can aid in configuring both firewalls and IDSs. Establishing a layered security architecture is advantageous whether an IDS is deployed or not. In addition to formulating a security policy, the essential steps consist of implementing user authentication and access controls, eliminating unnecessary services, applying patches to eliminate known vulnerabilities, deploying firewalls, using file integrity checking tools such as Tripwire, and so forth. Because most real-time commercial IDSs base their detection approach on known attempts to exploit known vulnerabilities, an administrator’s time is often better spent minimizing vulnerability through the application of patches or other security measures. Detecting and responding to penetration attempts that cannot succeed (such as Unix-specific at attempts against a network of
Windows machines) is not an effective use of resources, except as an indication of threat level. Using a network sensor outside the protected network lets the administrator sense the general threat level as indicated by probes and attempts that will be blocked by the outer firewall. Comparing the observations of sensors on both sides of the firewall lets the analyzer be configured to validate the firewall rules. The internal firewall provides an additional layer of defense for the inside workstations by excluding traffic that must reach the Web server from the outside but that should not reach the inside. In addition to helping to validate the inner firewall’s rules, it also protects the inside should the Web server be compromised and used as a base to attack the inside. If we assume that the protected enterprise is mission-oriented and only runs a limited set of applications and protocols, we can configure the inner sensor to recognize as intrusive any unexpected protocols. Host-based sensors on each workstation or server can look for both unexpected applications and abnormal behavior on the part of supported applications and the host operating system. When we combine the use of multiple firewalls and sensors configured to support a mission-specific security policy with a proactive vulnerability remediation policy, the removal of unneeded services, and the regular and careful use of integrity checking tools, the intruder’s task becomes much more difficult.

The IDS Life Cycle

9. Vendors frequently release new IDS products and aggressively compete for market share. Hiring and retaining personnel to competently administer security in general and intrusion detection in particular are increasingly challenging. Rapid changes in information technology make it difficult for an organization to implement an effective, long-term security strategy.

- **Evaluation and selection:** If an organization plans to acquire an IDS, it should consider the resources available for the system’s operation and maintenance and choose one than meets its needs within these constraints. This is difficult because there are no industry standards against which to compare IDSs. The new product cycle for commercial IDSs is rapid, and information and systems quickly become obsolete. IDS vendors usually specify which prototypical attacks their systems can find, but without access to deployment environments, they cannot describe how well their systems detect real attacks while avoiding false alarms. Topics to consider include detection and response characteristics, use of signature and anomaly-based approaches, diagnosis accuracy (false-alarm rate), ease of use, effectiveness of user interface, and quality of vendor support.

- **Deployment:** Issues to address include placement of sensors to maximize protection for the most critical assets, configuring the IDS to reflect security
policy, installing appropriate signatures and other initial conditions, establishing forensic procedures to preserve evidence for possible prosecutions, and determining when and what automatic responses are allowed. Users must develop procedures for handling IDS alerts and consider how to correlate alerts with other information such as system or application logs. Integrating the IDS into a comprehensive system management framework would simplify this latter task.

- **Operation and use:** Once an organization deploys an IDS, it must monitor the system and respond to the alerts that it reports. This means establishing roles and responsibilities for analyzing and acting on alerts, monitoring the outcomes of both manual and automatic responses, and so forth. IDSs themselves are logical targets for attack. Smart intruders who realize that an IDS has been deployed on a network their attacking is likely attack the IDS first, disabling it or forcing it to provide false information (distracting security personnel from the actual attack in progress). In addition, many commercial and research ID tools have security weaknesses resulting from flawed design assumptions. These can include failing to encrypt log files, omitting access control, and failing to perform integrity checks on IDS files.

- **Maintenance:** Activities include installing new signatures as they become available, as well as installing periodic IDS upgrades. Sensor placement should be revisited periodically to ensure that system or network changes have not reduced the effectiveness of the IDS. Use of technology alone is not sufficient to maintain network security. An organization must attract, train, and retain qualified technical staff to operate and maintain ID technologies.

- **Intrusion Detection Technology:** Commercial ID technology is immature and dynamic to the point of instability. New vendors appear, only to be absorbed by others. Both commercial and research products evolve rapidly. One consequence of this rapid change is that product lists, surveys, and a variety of commercial, research, and public domain ID tools are available.

**Commercial products**

10. Given today's volatile marketplace, it's best to use a Web search to locate current products, reviews, and so forth. Commercial product literature is generally weighted towards marketing, which often makes it difficult to determine the product's functionality and detection approach. Virtually no commercial literature addresses issues such as the frequencies of false alarms, missed detections, or the system's sensitivity to traffic loads.
RealSecure from Internet Security Systems (www.iss.net) is a real-time IDS that uses a three-part architecture consisting of a network-based recognition engine, a host-based recognition engine, and an administrator’s module. The network recognition engine runs on dedicated workstations to provide network intrusion detection and response. Each network-recognition engine monitors a network segment looking for packets that match attack signatures. When a network-recognition engine detects intrusive activity, it can respond by terminating the connection, sending alerts, recording the session, reconfiguring firewalls, and so forth. The host-based engines analyze log data to recognize attacks. Each host engine examines its system’s logs for evidence of intrusions and security breaches. Log data can contain information that is difficult or impossible to infer from network packet data. The host engine can prevent further incursions by terminating user processes or suspending user accounts. An administrative module manages multiple-recognition engines. The result is comprehensive protection, easily configured and administered from a single location. The administrative module is supplied with both recognition engines and is also available as a plug-in module for a variety of network and systems management environments.

Tripwire is a file integrity assessment tool (www.tripwire.com) that is useful for detecting the effects of an intrusion. Tripwire creates a database of critical system file information that includes file lengths and cryptographic checksums based on each file’s contents. Tripwire compares current information with a previously generated baseline and identifies changed files. Tripwire will report modified files, but the user must decide whether the modifications resulted from an intrusion. Because most monitored files are not expected to change except when new software versions are installed, changes usually indicate an unexpected or unauthorized activity. For reliable Tripwire results, users must protect the database and program from tampering, either by maintaining them offline or online using read-only storage media.

Shadow and Snort, two public-domain ID tools, are unlikely to have the same level of support as commercial systems, so users will need a higher level of technical expertise to install and manage them. The effort involved is likely to pay off with a better understanding of ID and its strengths and limitations. Sensors usually reside at key monitoring points in the network, such as outside a firewall, while the analysis station resides inside the firewall. The sensor is based on public domain packet-capture software and does not preprocess the data, thus preventing an intruder from determining the detection objectives by capturing an unprotected sensor. Sensors extract packet headers and save them to a file that the analysis station reads periodically. The analysis station uses a Web-based
interface to display filtering results as well as raw data. Shadow runs on many Unix systems and Linux.

Snort is a recent open-source public-domain effort to build a lightweight, efficient, ID tool that can be deployed on a wide variety of Unix platforms. According to the Snort Web site (www.snort.org), views are quickly outdated. The “Technology” sidebar describes a sample of commercial, research, and public domain tools. Snort is a lightweight network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis, content searching/matching and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more. Snort uses a flexible rules language to describe traffic that it should collect or pass, as well as a detection engine that utilizes a modular plugin architecture. Snort is currently undergoing rapid development. The user community is contributing auxiliary tools for analyzing and summarizing snort logs, providing additional capabilities. More importantly, there is a large group of users who contribute new signatures. As a result, new attacks are quickly represented in the signature database.

**Conclusion**

11. Intrusion detection systems (IDSs) attempt to identify computer system and network intrusions and misuse by gathering and analyzing data. IDSs have traditionally been developed to detect intrusions and misuse for wired systems and networks. More recently, IDSs have been developed for use on wireless networks. These wireless IDSs can monitor and analyze user and system activities, recognize patterns of known attacks, identify abnormal network activity, and detect policy violations for WLANs. Wireless IDSs gather all local wireless transmissions and generate alerts based either on predefined signatures or on anomalies in the traffic.

12. Intrusion detection systems are an important addition to the security of wireless local area networks. While there are drawbacks to implementing a IDS, the benefits will most likely prove to outweigh the downsides. With the capability to detect probes, in addition to assistance with policy enforcement, the benefits of a wireless IDS can be substantial. Of course, just as with a wired network, an IDS is only one part of a greater security solution wireless network. WLANs require a number of other security measures to be employed before an adequate level of security can be reached, but the addition of a wireless IDS can greatly improve the security posture of the entire network. With the immense rate of wireless adoption, the ever-increasing number of threats to WLANs, and the growing complexity of attacks, a system to identify and report on threat information can greatly enhance the security of a wireless network.