CHAPTER 5 Detection

LEARNING OUTCOMES

By the end of this chapter, you should be able to:

1. Determine the meaning of vulnerability and intrusion detection;
2. Identify the cause of the vulnerability;
3. Describe the different types of Intrusion Detection Systems;
4. Identify the usage of monitor and control in detection system; and
5. Understand the usage of application control.

INTRODUCTION

Observe the newspaper article below by BERNAMA.

Cyber Security Incidents Increasing, Says MOSTI

KUALA LUMPUR, July 7 (Bernama) -- Cyber security incidents reported from January to May this year increased by about 25 percent to 1,247 compared with the same period last year.

Science, Technology and Innovation (MOSTI) Deputy Minister, Fadillah Yusof, said the figure has exceeded by more than 50 percent on a year-on-year basis.

"In 2008, 2,123 cases were reported. The increase was due to greed or ignorance.

"These were incidents that have been categorised as intrusion, use of malicious code, fraud, harassment and spam," he said after the launch of the Cyber Security Malaysia SecureAsia@Kuala Lumpur Conference and Exhibition here on Tuesday.

The deputy minister also launched the Cyber999 Help Centre, a "cyber incident" response centre for the public to report Internet-related problems.

The 24-hour Cyber999 service is provided and managed by Cybersecurity Malaysia, the national cybersecurity specialist under the purview of Mosti.

The public can call 1300 88 2999, e-mail cyber999@cybersecurity.my or surf to www.cybersecurity.my.

Earlier, Fadillah said it was imperative that countries around the world work in concert to manage these cyber threats as many of the computer systems, whether in the government or private organisations, were interconnected.

"We must work collectively as partners to secure the information networks, systems and infrastructures that drive our country's economic activity," he said at the opening of the conference and exhibition.

The event was jointly organised by Cyber Security Malaysia and the International Information Systems Security Certification Consortium, or (ISC)2, a non-profit organisation headquartered in Palm Harbor, Florida.

The conference and exhibition provides a platform for the public to take stock of the opportunities and threats brought about by information security.

At the event, CyberSecurity Malaysia also exchanged memorandum of understandings (MOUs) with Malaysia Airlines, Asia e-University, Centre for Advance Software Engineering of Universiti Teknologi Malaysia, Management Science University and Mimos Bhd.

The MOU, among others, focuses on various information and communication technologies (ICT) security initiatives including talent capital development, establishing general digital forensic framework, e-learning development and ICT security innovation.

-- BERNAMA

Source: http://www.bernama.com/bernama/v5/newsindex.php?id=423574

From the article above, highlight the causes and the action taken to overcome this matter. In your opinion, what solutions can be made to curb these cyber security incidents?

Share your opinions in the LMS Forum.

No matter what level of protection, security incidents will occur and systems will fail, and detection is the only way of knowing when the system is compromised. This is why rapid detection and appropriate notification are the most important parts of any security strategy. Intrusion detection is the act of detecting actions that attempt to compromise the confidentiality, integrity or availability of a resource.

Without proper detection, you may never be aware that a security incident has occurred and thereby continue to use corrupt information to make business decision.

5.1 VULNERABILITY AND INTRUSION DETECTION

Source: http://www.youtube.com/watch?v=RoB0mLerbG0

The video shows about Intrusion Detection In-Depth. From the tutorial video given, identify what Intrusion Detection is.

5.1.1 What is Vulnerability?

In computer security, the term vulnerability is applied to a weakness in a system which allows an attacker to violate the integrity of that system. Vulnerabilities may result from (see Figure 5.1).

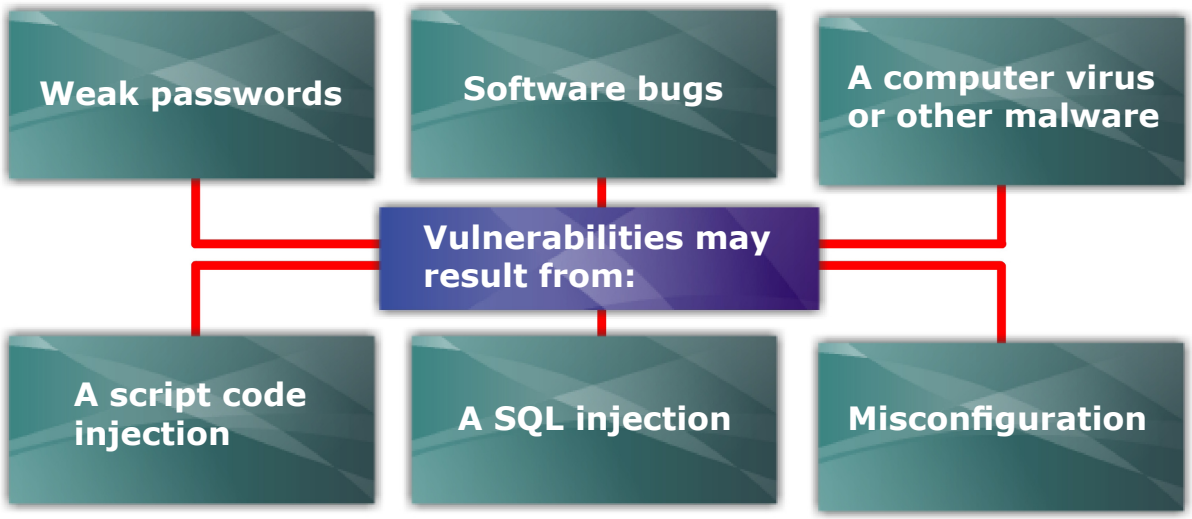


Figure 5.1: Examples of results from vulnerabilities

A security risk is classified as vulnerability if it is recognised as a possible means of attack. A security risk with one or more known instances of working and fully-implemented attacks is classified as an exploit. Constructs in programming languages that are difficult to use properly can be a large source of vulnerabilities.

5.1.2 What is the Cause of Vulnerability?

Some of the causes of vulnerability is as shown in Table 5.1.

Table 5.1: Causes of Vulnerability

Flaws	Example of flaws
Password Management	• The computer user uses weak passwords that could be discovered by brute force. • The computer user stores the password on the computer where a program can access it. • Users reuse passwords between many programs and web-sites.
Fundamental Operating System Design	• The operating system designer chooses to enforce sub optimal policies on user/program management. For example operating systems with policies such as default permit grant every program and every user full access to the entire computer. This operating system flaw allows viruses and malware to execute commands on behalf of the administrator.

Software Bugs	• The programmer leaves an exploitable bug in a software program. The software bug may allow an attacker to misuse an application.
Unchecked User Input	• The program assumes that all user input is safe. Programs that do not check user input can allow unintended direct execution of commands or SQL statements (known as Buffer overflows, SQL injection or other non-validated inputs).

5.1.3 How to Remove the Vulnerability?

Many software tools exist that can aid in the discovery or removal of vulnerabilities in a computer system. Though these tools can provide an auditor with a good overview of possible vulnerabilities present, they cannot replace human judgment. Relying solely on scanners will yield false positives and a limited-scope view of the problems present in the system.

Vulnerabilities have been found in every major operating system including Windows, Mac OS, various forms of UNIX and Linux, OpenVMS, and others.

Figure 5.2 describe the ways to reduce the chance of a vulnerability being used against a system.

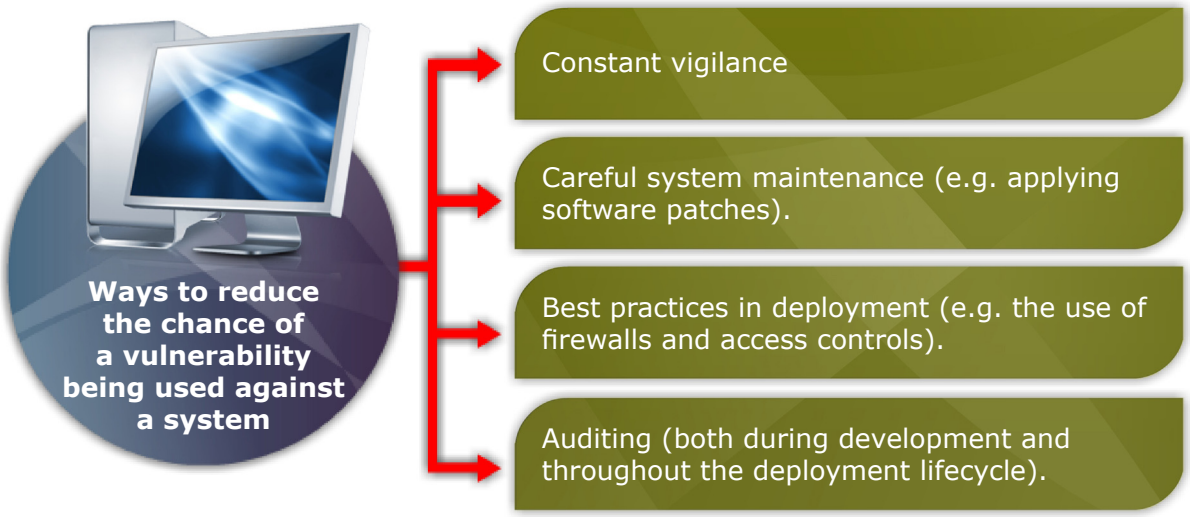


Figure 5.2: Ways to reduce the chance of a vulnerability being used against a system

5.1.4 What is Intrusion Detection?

In Information Security, Intrusion Detection (ID) is the act of detecting actions that attempt to compromise the confidentiality, integrity or availability of a resource. The goal of intrusion detection is to identify entities attempting to subvert in –place security controls. When intrusion detection takes a preventive measure without direct human intervention, then it becomes an intrusion-prevention system.

Intrusion detection (ID) is a type of security management system for computers and networks (see Figure 5.3).

An ID system gathers and analyses information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organisation) and misuse (attacks from within the organisation).

ID uses vulnerability assessment (sometimes referred to as scanning), which is a technology developed to assess the security of a computer system or network.

Figure 5.3: How intrusion detection works

Intrusion detection functions include:

- Monitoring and analysing both user and system activities;
- Analysing system configurations and vulnerabilities;
- Assessing system and file integrity;
- Ability to recognise patterns typical of attacks;
- Analysis of abnormal activity patterns; and
- Tracking user policy violations.

ID systems are being developed in response to the increasing number of attacks on major sites and networks, including those of the Pentagon, the White House, NATO, and the U.S. Defense Department.

The safeguarding of security is becoming increasingly difficult, because the possible technologies of attack are becoming ever more sophisticated; at the same time, less

technical ability is required for the novice attacker, because proven past methods are easily accessed through the Web.

Intrusion detection can be performed manually or automatically, as shown in Figure 5.4.

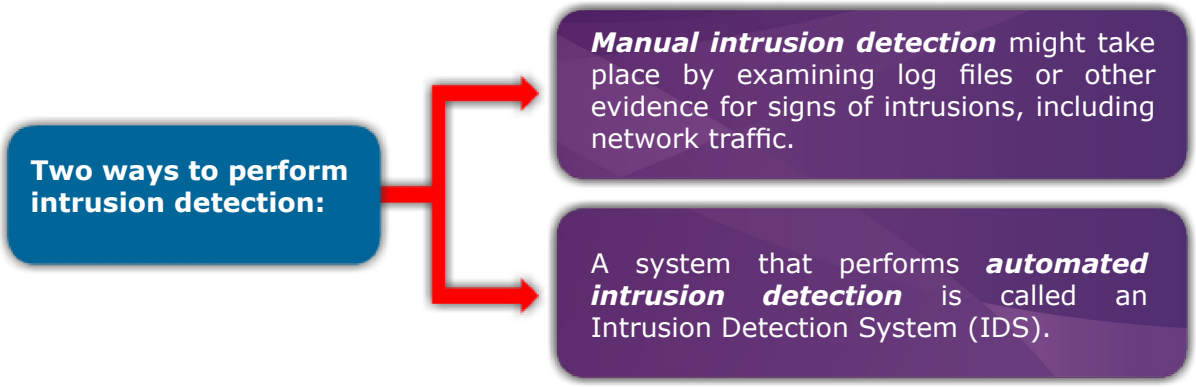


Figure 5.4: Two ways to perform intrusion detection

An IDS can be either host-based, if it monitors system calls or logs, or network-based if it monitors the flow of network packets. Modern IDSs are usually a combination of these two approaches. Another important distinction is between systems that identify patterns of traffic or application data presumed to be malicious (misuse detection systems), and systems that compare activities against a 'normal' baseline (anomaly detection systems).

When a probable intrusion is discovered by IDS, typical actions to perform would be logging relevant information to a file or database, generating an email alert, or generating a message to a pager or mobile phone. Determining what the probable intrusion actually is and taking some form of action to stop it or prevent it from happening again are usually outside the scope of intrusion detection.

However, some forms of automatic reaction can be implemented through the interaction of Intrusion Detection Systems and access control systems such as firewalls. Some researchers classify the identification of attack attempts at the source system as extrusion detection (also known as outbound intrusion detection) techniques. Intrusion prevention is an evolution of intrusion detection.

5.1.5 Common Types of Intrusion Detection

There are four common types of Intrusion Detection. These common types are described in Figure 5.5.

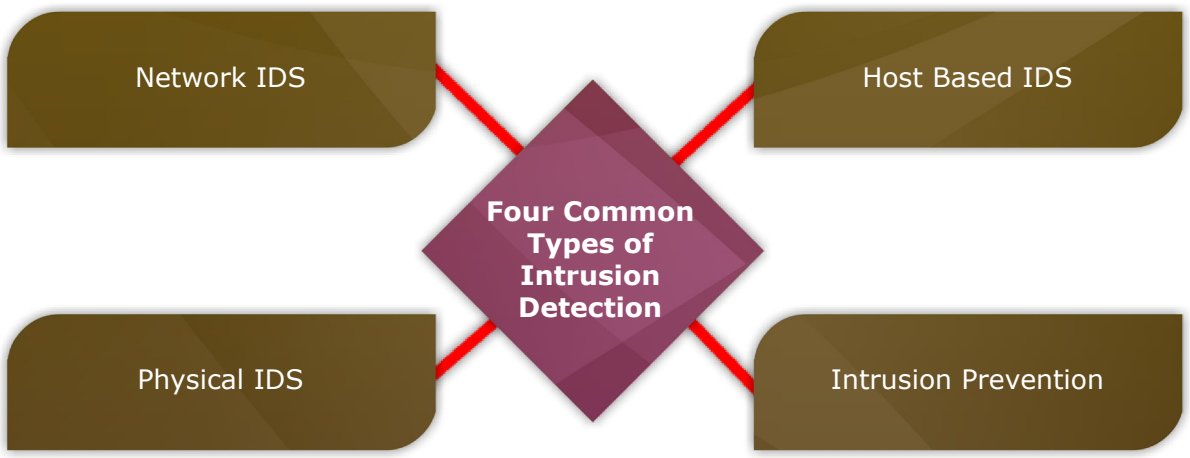


Figure 5.5: Four common types of intrusion detection

From Figure 5.5, we will elaborate each if the function as below:

(a) **Network Based (Network IDS)**

Network based intrusion detection attempts to identify unauthorised, illicit, and anomalous behavior based solely on network traffic. A network IDS, using either a network tap, span port or hub collects packets that traverse a given network. Using the captured data, the IDS system processes and flags any suspicious traffic. Unlike an intrusion prevention system, an intrusion detection system does not actively block network traffic.

The role of a network IDS is passive, only gathering, identifying, logging and alerting. Example of Network IDS is SNORT.

(b) **Host Based (HIDS)**

Often referred to as HIDS, host based intrusion detection attempts to identify unauthorised, illicit, and anomalous behavior on a specific device. HIDS generally involves an agent installed on each system, monitoring and alerting on local OS and application activity. The installed agent uses a combination of signatures, rules, and heuristics to identify unauthorised activity. The role of a host IDS is passive, only gathering, identifying, logging, and alerting. Examples of HIDS:

- **OSSEC** - Open Source Host-based Intrusion Detection System.
- **Tripwire**
- **AIDE** - Advanced Intrusion Detection Environment.
- **Prelude Hybrid IDS**

(c) **Physical (Physical IDS)**

Physical intrusion detection is the act of identifying threats to physical systems. Physical intrusion detection is most often seen as physical controls put in place to ensure CIA.

In many cases physical intrusion detection systems act as prevention systems as well. Figure 5.6 shows examples of physical intrusion detection.

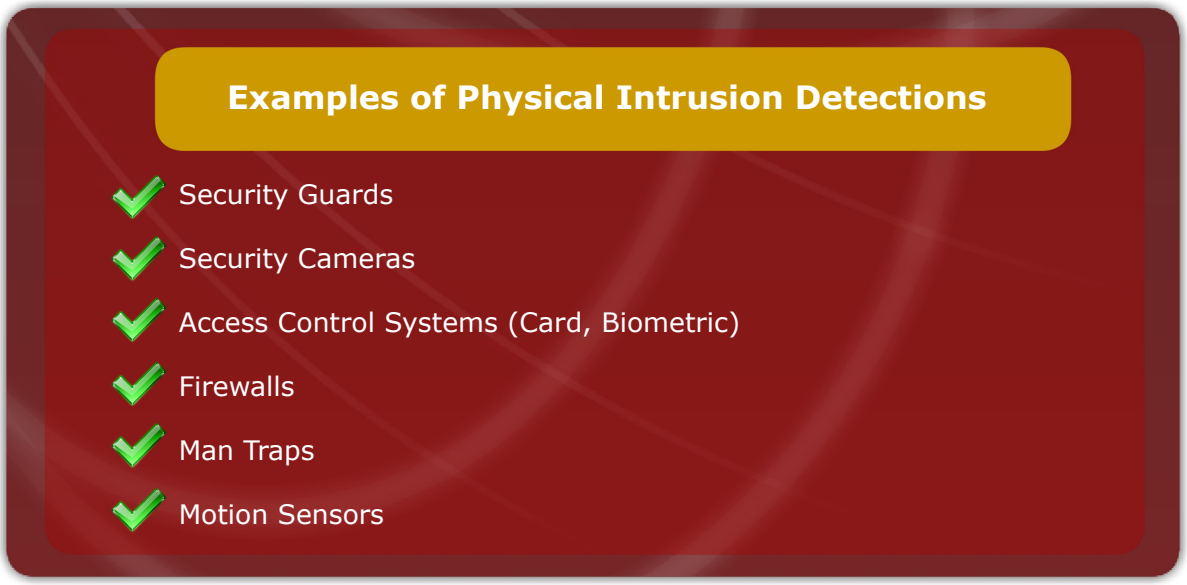


Figure 5.6: Examples of physical intrusion detection

(d) **Intrusion Prevention**

Intrusion prevention follows the same process of gathering and identifying data and behavior, with the added ability to block (prevent) the activity. This can be done with Network, Host, and Physical Intrusion Detection Systems.

5.1.6 Intrusion Detection System

An Intrusion Detection System (IDS) is a device or software tools or hardware tools that monitor activity to identify malicious or suspicious events. IDS also used to detect unauthorised access to a computer system or network. This may take the form of attacks by skilled malicious hackers, or script kiddies using automated tools. An example of intrusion detection system is displayed in Figure 5.7.

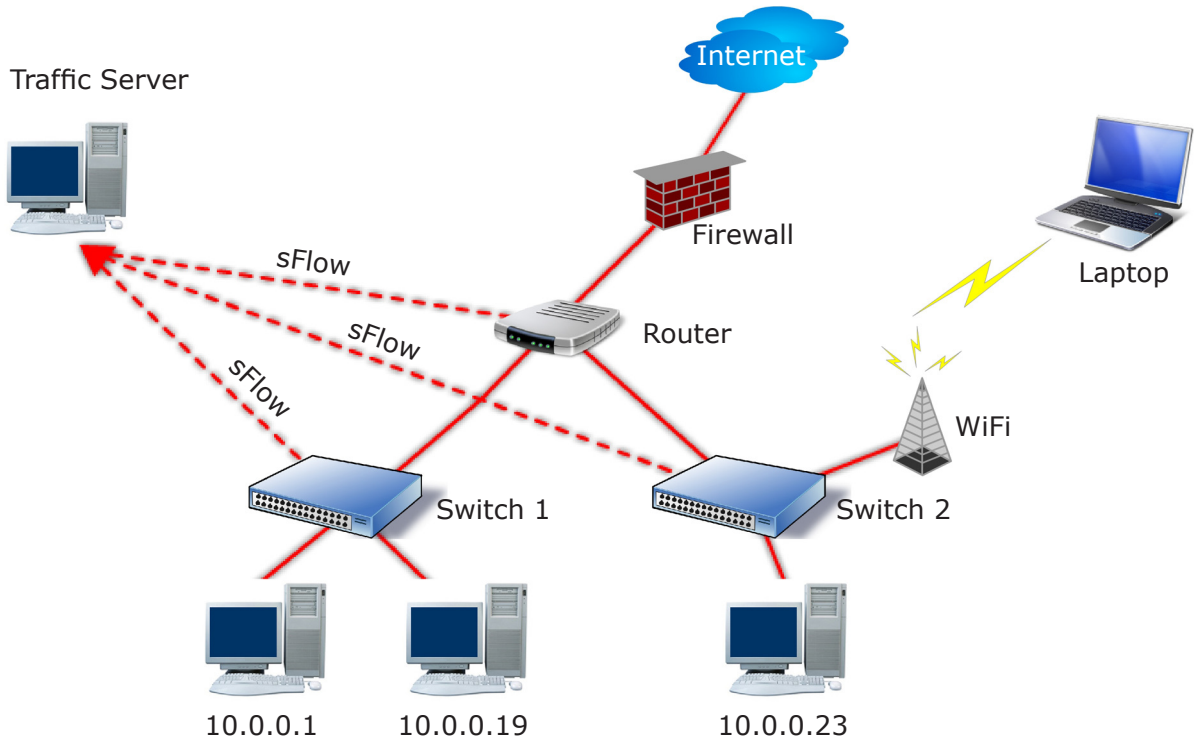


Figure 5.7: An example of intrusion detection system

An IDS is required to detect all types of malicious network traffic and computer usage. This includes:

- Network attacks against vulnerable services;
- Data driven attacks on applications;
- Host based attacks such as privilege escalation;
- Unauthorised logins and access to sensitive files; and
- Malware (viruses, Trojan horses, and worms).

An IDS is composed of several components, Sensors which generate security events, a Console to monitor events and alerts and control the sensors, and a central Engine that records events logged by the sensors in a database and uses a system of rules to generate alerts from security events received. There are several ways to categories an IDS depending on the type and location of the sensors and the methodology used by the engine to generate alerts. In many simple IDS implementations all three components are combined in a single device or appliance.

A model of an IDS is shown in Figure 5.8.

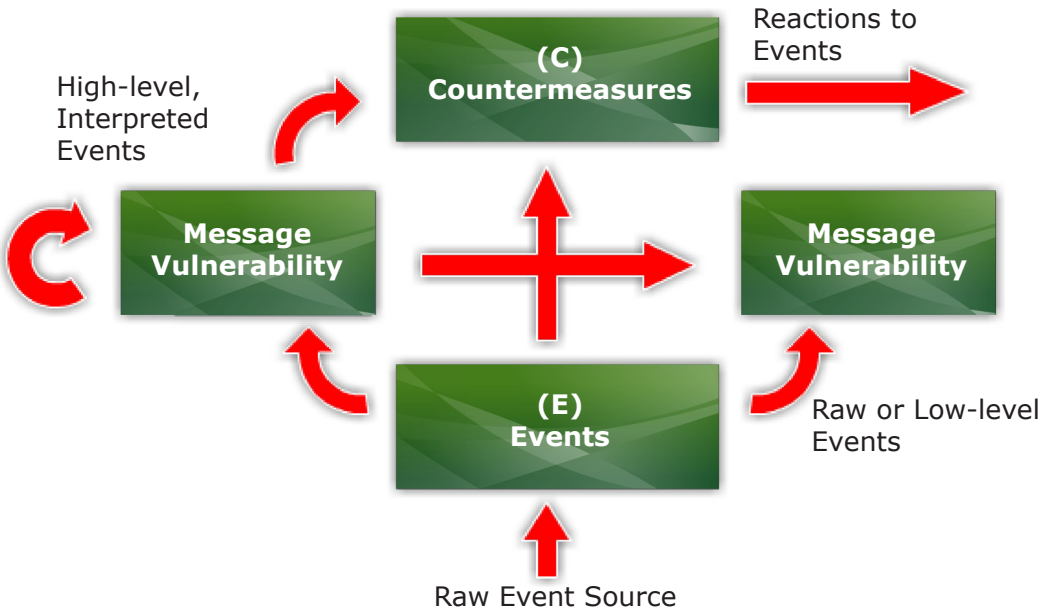


Figure 5.8: Common components of an intrusion detection framework

The components in the figure are the four basic elements of an intrusion detection systems based on the Common Intrusion Detection Framework of Stanford research in his proceeding paper at Pro National Information Systems Security Conference. An IDS receives raw inputs from sensors. It saves those inputs, analyses them and takes some controlling action.

- An IDS performs a variety of functions which are:
- Monitoring users and system activity;
- Auditing system configuration for vulnerabilities and misconfigurations;
- Assessing the integrity of critical system and data files;
- Recognising known attack patterns in system activity;
- Identifying abnormal activity through statistical analysis;
- Managing audit trails and highlighting user violation of policy or normal activity;
- Correcting system configuration errors; and
- Installing and operating traps to record information about intruders.

5.1.6.1 Types of Intrusion Detection Systems (IDS)

Two general types of intrusion detection systems are displayed in Figure 5.9.

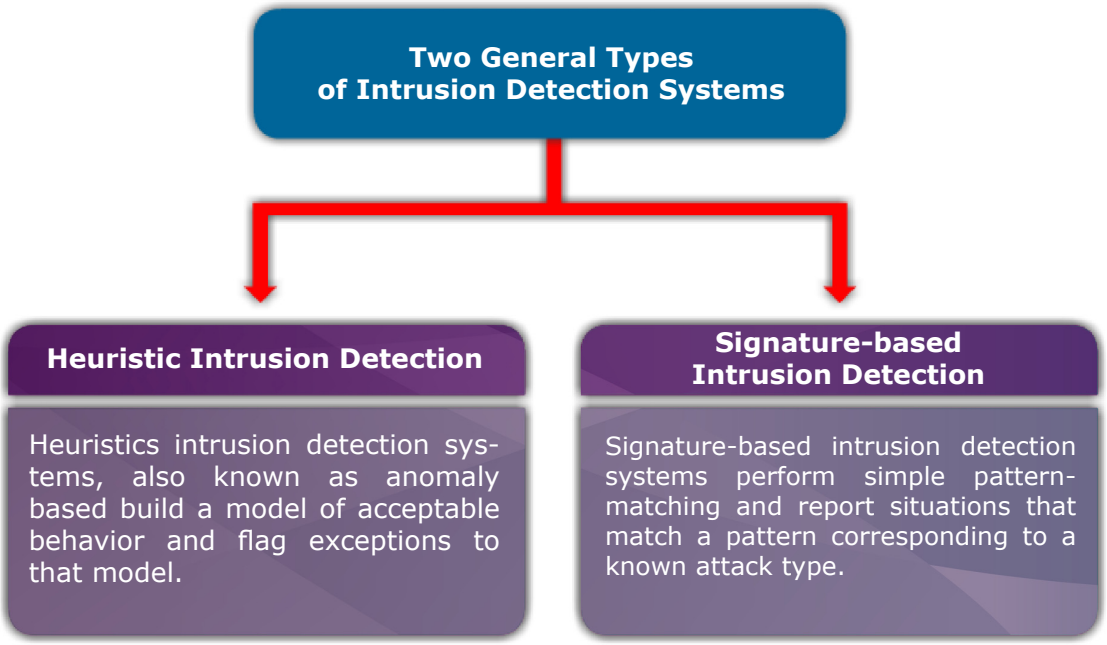


Figure 5.9: Two general types of intrusion detection systems

Intrusion detection devices can be network based or host based. A network based IDS is a stand-alone device attached to the network to monitor traffic throughout that network. A host-based ID runs on a single workstation, client or host to protect another host.

(a) **Misuse Detection vs. Anomaly Detection**

A misuse detection system, also known as a ***Signature-Based Intrusion Detection System*** identifies intrusions by watching for patterns of traffic or application data presumed to be malicious. These types of systems are presumed to be able to detect only 'known' attacks. However, depending on their rule set, signature-based IDSs can sometimes detect new attacks which share characteristics with old attacks, e.g., accessing 'cmd.exe' via a HTTP GET request.

The IDS analyses the information it gathers and compares it to large databases of attack signatures. Essentially, the IDS look for a specific attack that has already been documented. Like a virus detection system, misuse detection software is only as good as the database of attack signatures that it uses to compare packets against.

An ***Anomaly-Based Intrusion Detection System*** identifies intrusions by notifying operators of traffic or application content presumed to be different from 'normal' activity on the network or host. Anomaly-based IDSs typically achieve this with self-learning.

An Anomaly-Based Intrusion Detection System is a system for detecting computer intrusions and misuse by monitoring system activity and classifying it as either

Normal or ***Anomalous***. The classification is based on heuristics or rules, rather than patterns or signatures, and will detect any type of misuse that falls out with normal system operation. This is as opposed to signature based systems which can only detect attacks for which a signature has previously been created.

In order to determine what attack traffic is, the system must be taught to recognise normal system activity. This can be accomplished in several ways, most often with Artificial Intelligence type techniques. Systems using Neural Networks have been used to great effect. Another method is to define what normal usage of the system comprises using a strict mathematical model, and flag any deviation from this as an attack. This is known as ***Strict Anomaly Detection***.

In anomaly detection, the system administrator defines the baseline, or normal, state of the network's traffic load, breakdown, protocol, and typical packet size. The anomaly detector monitors network segments to compare their state to the normal baseline and look for anomalies.

(b) **Network-based vs. Host-based Systems**

In a network-based system, or NIDS, the sensors are located at choke points in the network to be monitored, often in the DMZ or at network borders. The sensor captures all network traffic flows and analyses the content of individual packets for malicious traffic. In a host-based system, the sensor usually consists of a software agent which monitors all activity of the host on which it is installed. Hybrids of these two types of system also exist.

Table 5.2 below describes the types of intrusion detection system.

Table 5.2: Types of Intrusion Detection Systems

Types of Intrusion Detection System	Description
Network Intrusion Detection System	• An independent platform which identifies intrusions by examining network traffic and monitors multiple hosts. • Network Intrusion Detection Systems gain access to network traffic by connecting to a hub, network switch configured for port mirroring, or network tap. An example of a NIDS is Snort.
Host-based Intrusion Detection System	• A **Host-based Intrusion Detection System** consists of an agent on a host which identifies intrusions by analysing system calls, application logs, file-system modifications (binaries, password files, capability/acl databases) and other host activities and state.

Host-based Intrusion Detection System	• A **Host-based Intrusion Detection System** combines both approaches. • Host agent data is combined with network information to form a comprehensive view of the network. An example of a Hybrid IDS is Prelude.

(c) **Passive System vs. Reactive System**

In a **passive system**, the IDS sensor detects a potential security breach, logs the information and signals an alert on the console. In a **reactive system**, the IDS respond to the suspicious activity by logging off a user or by reprogramming the firewall to block network traffic from the suspected malicious source, either autonomously or at the command of an operator.

Though they both relate to network security, an IDS differs from a firewall in that a firewall looks out for intrusions in order to stop them from happening. The firewall limits the access between networks in order to prevent intrusion and does not signal an attack from inside the network. An IDS evaluates a suspected intrusion once it has taken place and signals an alarm. An IDS also watches for attacks that originate from within a system.

This is traditionally achieved by examining network communications, identifying heuristics and patterns (often known as signatures) of common computer attacks, and taking action to alert operators.

A system which terminates connections is called an ***Intrusion-Prevention System***, and is another form of an application layer firewall.

5.1.6.2 Intrusion Detection Systems (IDS) Strengths and Limitations

Although Intrusion Detection Systems are a valuable addition to an organisation's security infrastructure, there are things they do well, and other things they do not do well. As you plan the security strategy for your organisation's systems, it is important for you to understand what IDSs should be trusted to do and what goals might be better served by other types of security mechanisms.

(a) **Strengths of Intrusion Detection Systems**

Intrusion detection systems perform the following functions as shown in Figure 5.10.

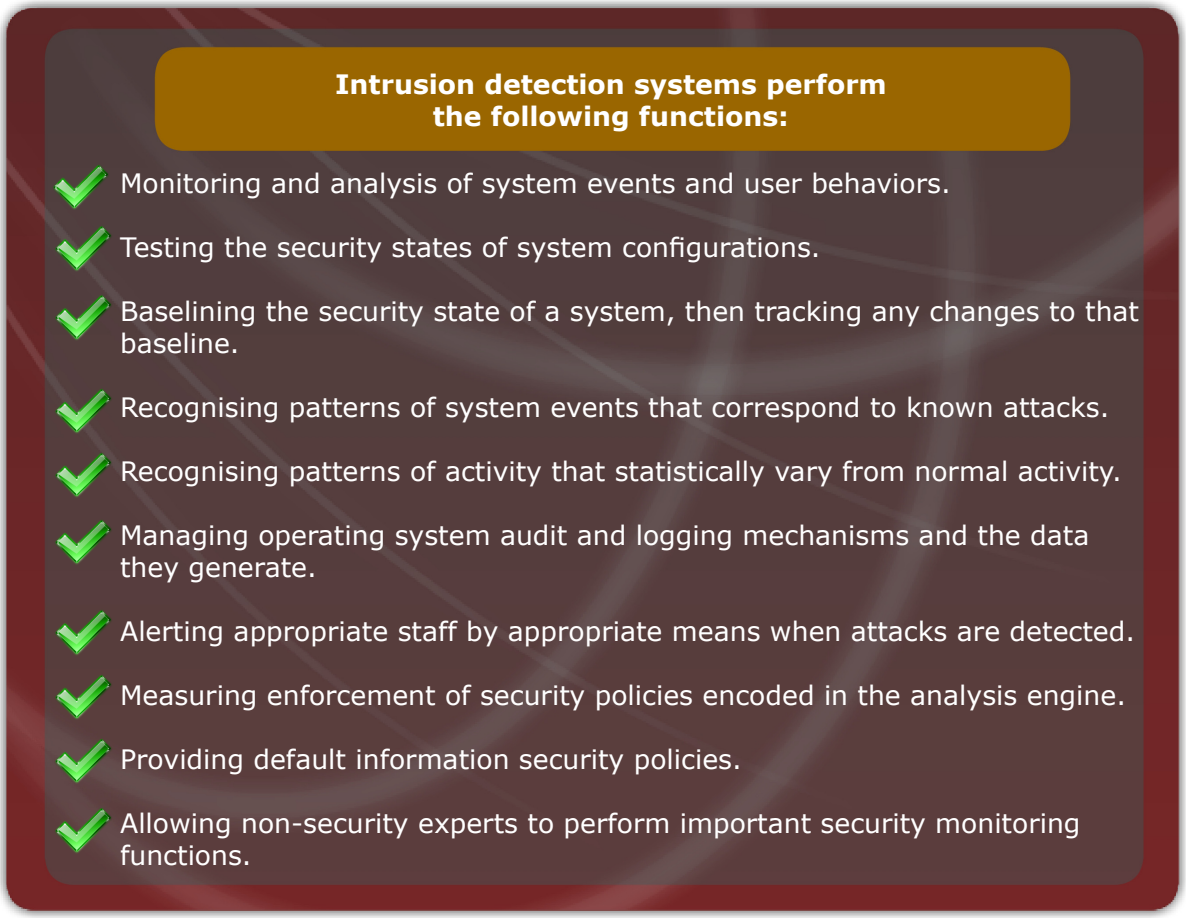


Figure 5.10: How intrusion detection systems perform

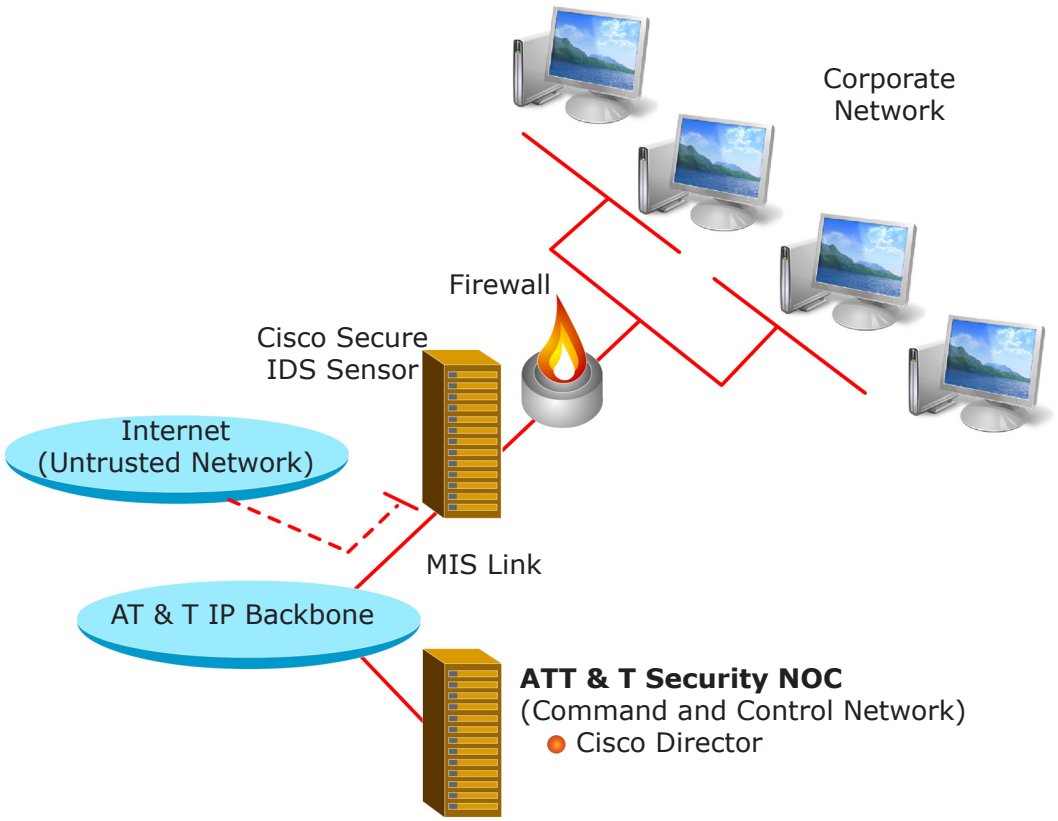
(b) **Limitations of Intrusion Detection Systems**

Intrusion detection systems cannot perform the following functions:

- Compensating for weak or missing security mechanisms in the protection infrastructure. Such mechanisms include firewalls, identification and authentication, link encryption, access control mechanisms, and virus detection and eradication.
- Instantaneously detecting, reporting, and responding to an attack, when there is a heavy network or processing load.
- Detecting newly published attacks or variants of existing attacks.
- Effectively responding to attacks launched by sophisticated attackers.
- Automatically investigating attacks without human intervention.
- Resisting attacks that are intended to defeat or circumvent them.
- Compensating for problems with the fidelity of information sources.
- Dealing effectively with switched networks.

5.2 MONITORING AND CONTROL

Once the organisation deploy and depend upon data networks, it must assume the responsibility to monitor and control activity on the networks.



Network intrusion monitoring is observing the actions, security logs, or audit data of the network for attempts by outsiders or insiders to compromise the integrity, confidentiality or availability of organisational resources. Due to the increasing shortage of network security personnel, staffing budget constraints or a false sense of security, many organisations neglect this critical aspect of creating a secure environment.

Procedures should be in place to constantly monitor the logs, messages, and alarms from all your systems – application servers, operating systems, network routers, firewalls, VPN servers, remote access servers, and host and network based intrusion detection systems. You have to ensure that you don't miss any innocuous looking message or alarm that signals an intrusion. Constant intrusion monitoring should be an integral part of the security process.

Each organisation should begin formulating their monitoring policy by defining what type of event will constitute an intrusion. This definition will come as a result of evaluating and identifying the security risks within the organisation. The next step is to establish the monitoring practices that can help identify these intrusions and how

each incident will be handled. In a well-secured network, intrusions will happen sporadically.

There are significant intervals of time when there is no unusual activity and, as any night watchman will tell you, it's easy to fall asleep. Since intrusion monitoring is where you spend most of your time after your security framework is up and functional, it's essential that the monitoring practices be well-defined, documented, and periodically reviewed.

5.2.1 Infrastructure Should be Monitored

Each organisation should identify the devices, applications and processes specific to the systems they want to monitor. Facets of the network that should be evaluated include:

- Network, System and Application Logs;
- System Processes;
- Utilisation of Networks, CPUs and Disks;
- Configuration Integrity of Network Devices, Operating Systems and Applications;
- Version Integrity of Network Devices, Operating Systems and Applications; and
- Vulnerability of Networks and Devices.

A wealth of information directly available from systems on the organisation's network that can raise flags even if your intrusion detection system doesn't detect an intrusion. These logs are very useful when investigating an intrusion and can be used as evidence by law enforcement agencies to prosecute intruders. The logs from these various devices must be evaluated and configured in a consistent manner. In some systems these logs are stored in a database for log-reduction analysis.

Logs (see Figure 5.11) can be derived from:

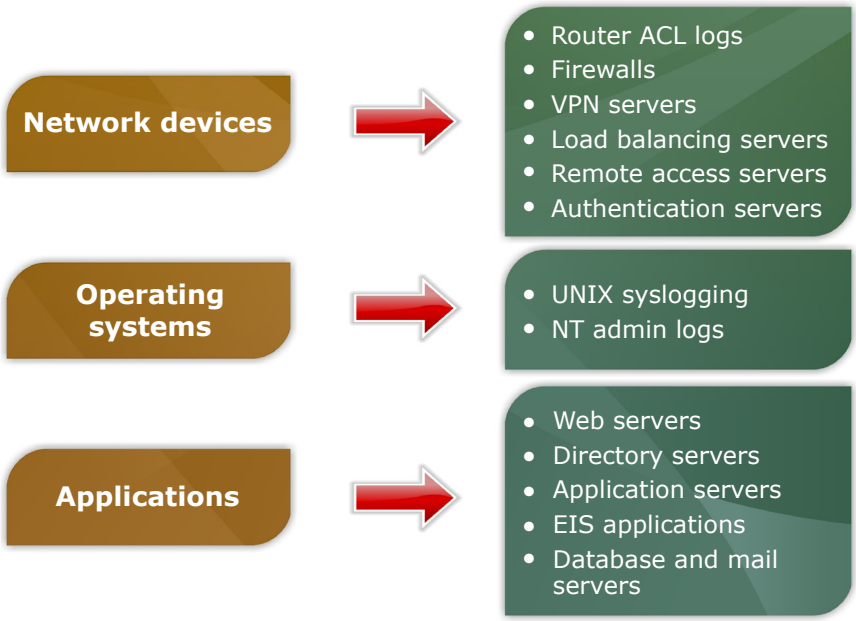


Figure 5.11: Three examples of where logs derived from

There are a number of other network components that could be monitored periodically to get advance notice of suspicious activity which are showed in Table 5.3.

Table 5.3: Examples of Network Components That Could Get Advance Notice of Suspicious Activity

Network Components	Description
Processes on critical servers	• Check for availability of critical processes and scan the process table for unknown processes. • Verify the count of processes on a system against an average threshold. A significant difference could indicate an intrusion.
Configuration	• Create integrity hashes for all network, system, and application configuration files and periodically check them.
Utilisation	• Check CPU, disk, and network utilisation for unusual patterns including high usage at odd times.
Site	• Specific components to identify anomalies against the regular usage patterns.

5.2.2 Monitoring Techniques

There are three techniques that can be used for monitoring the intrusion. The monitoring can be used one of the techniques or a combination of the techniques. The most common method is audit trail processing. Although it is considered "after-the-fact" analysis, it is helpful in assessing damage that may have been done to the protected assets and track the complete footprint of an intruder's activity.

Near real-time processing depends on the type of intrusion detection system that is used. IDS systems can be classified based on monitoring methods:

- Monitoring the patterns and profiles of normal behavior.
- Monitoring patterns of misuse, known attack signatures and suspicious attack patterns.
- Monitoring based on pattern matching (operation experience).

The Periodic Assessment method of intrusion monitoring involves activities like vulnerability scanning, network audits, system and application audits. These assessments are often used periodically to revise the organisations security policies and procedures. Tools that are used in periodic assessment include (see Figure 5.12).

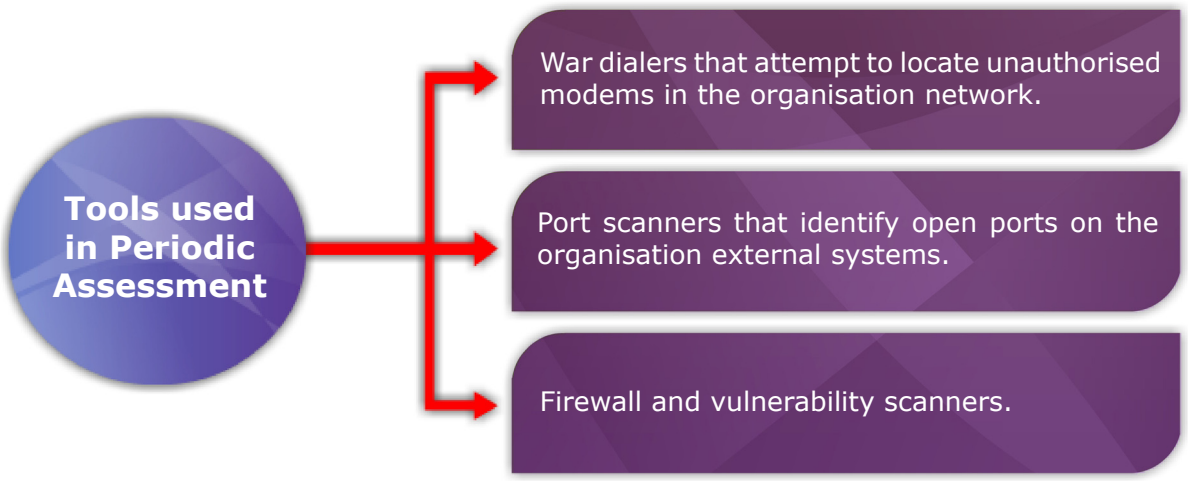


Figure 5.12: Tools that are used in periodic assessment

Proactive monitoring prevents potential damage to protected assets by taking appropriate action before an intrusion occurs. Based on predictive analysis, this technology is still evolving and has yet to be stabilised. IDS vendors will need to standardise reporting and logging formats to make this a viable method of monitoring.

Using near real-time monitoring, intrusion activity can be tracked in real-time and decisions can be made quickly to avoid potential damage to protected assets. Automated responses can be taken based on attack profiling, which has been developed over a period of time.

Audit trail analysis can be helpful in assessing damage that may have been done to protected assets. It is also used to track the activity of an intruder and gather a footprint that may be used in prosecution. This type of historical analysis is also useful in revising organisational security policies and procedures.

5.3 APPLICATION CONTROL

In business and accounting, **Information technology controls** (or **IT controls**) are specific activities performed by persons or systems designed to ensure that business objectives are met. They are a subset of an enterprise's internal control. IT control objectives relate to the confidentiality, integrity, and availability (CIA) of data and the overall management of the IT function of the business enterprise.

IT controls are often described in two categories as shown in Figure 5.13.

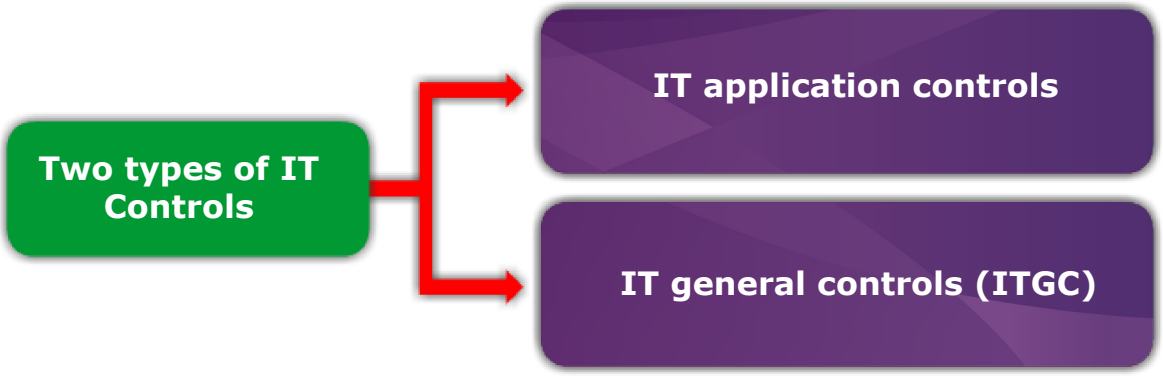


Figure 5.13: Two types of IT Controls

(a) **IT general controls (ITGC)**

ITGC include controls over the information technology (IT) environment, computer operations, access to programs and data, program development and program changes.

(b) **IT application controls**

It refers to transaction processing controls, sometimes called "input-processing-output" controls. IT application or program controls are fully-automated (i.e., performed automatically by the systems) designed to ensure the complete and accurate processing of data, from input through output.

IT application control provides granular, policy-based enforcement of application use to proactively secure endpoints from data leakage, malware, spyware, keyloggers, Trojans, rootkits, worms and viruses, zero-day threats and unwanted or unlicensed software. These controls vary based on the business purpose of the specific application. These controls may also help ensure the privacy and security of data transmitted between applications.

Categories of IT application controls may include:

- **Completeness checks** - Controls that ensure all records were processed from initiation to completion.
- **Validity checks** - Controls that ensure only valid data is input or processed.
- **Identification** - Controls that ensure all users are uniquely and irrefutably identified.
- **Authentication** - Controls that provide an authentication mechanism in the application system.
- **Authorisation** - Controls that ensure only approved business users have access to the application system.

Application control and its sidekick device control are making inroads in the corporate world for protecting managed desktops and servers. Application control steps in whenever a user launches an executable to issue an "approved" or not "approved" verdict. The technology works alongside traditional anti-virus, personal firewall, and intrusion

prevention products for IT to control endpoint activity.

The primary motivation for deploying application control is that applications installed from unofficial sources are more likely to contain malicious code that can disrupt business operations or steal confidential information. Other application control benefits include restricting use of non-business applications (such as media players) to improve network performance or comply with HR guidelines, and managing endpoint configurations to enhance security and reduce help desk calls.

Typically application control as described in Table 5.4 relies on some variant of IT established approaches that are checked when a user launches an application.

Table 5.4: Typically Application Control That Relies on Some Variant of IT Established Approaches

Typically Application Control	Description
White-list	• A **white-list** is a list of all the applications that users are explicitly allowed to execute. • IT controls this list of permissible applications that have been vetted for security and business justification.
Black-list	• A **black-list** is a list of all the applications that users are forbidden to run. • IT places executables on the black-list when they are associated with malware or unauthorised uses of corporate resources.
Grey-list	• A **grey-list** is everything in between white and black lists. If application control cannot identify the application. • Then the user may place the application on a grey-list with extra auditing vigilance enabled so IT can make a subsequent yes or no decision.

Implementing application control in an administrative-friendly way is more challenging, as the lists can become quite large for all the various user profiles. Good approaches are mindful of users needing to self-provision applications before IT can centrally approve them, normal IT operations requirements for software upgrades and patches, executable libraries that multiple applications use and comprehensive reporting to please the compliance auditors.

Application control is an interesting approach for organisations looking for automated tools to help exercise tighter management of endpoints. Companies that specialise in application control are shown in Figure 5.14. They are well worth checking out as good complements to identity-based access control and anti-malware products.

Figure 5.14: Examples of companies that specialise in application control

Some of the advantages in implementing certain application control are:

- Eliminates the reliance on anti-virus subscription updates to secure business.
- Enforces software license compliance, Sarbanes Oxley, HIPAA and GLBA and many other regulatory requirements.
- Enables application monitoring to avoid propagation of illegal, malicious or unwanted code on endpoints.
- Prevents unauthorised application use throughout the organisation.
- Allows to test and plan patch deployment with no rush.
- Benefit from Standard File Definitions to rapidly load a predefined set of authorised OS and most commonly used applications.

SUMMARY

1. Vulnerability is applied to a weakness in a system which allows an attacker to violate the integrity of that system. Some of the flaws is due to the password management flaws, fundamental OS design, software bugs and unchecked user input.
2. **Intrusion detection** is the act of detecting actions that attempt to compromise the confidentiality, integrity or availability of a resource.
3. There are four common types of Intrusion Detection which are Network IDS, Host Based IDS, Physical IDS and Intrusion Prevention.
4. IT application or program controls are fully-automated designed to ensure the complete and accurate processing of data, from input through output.

GLOSSARY

CIA	Confidential, Integrity and Availability.
Defense	A means or method of defending or protecting.
IDS	Intrusion Detection System.
Information Infrastructure	The entirety of IT elements that are part of a given infrastructure.
IT	Information Technology
Technical	Having special skill or practical knowledge.

DISCUSSION QUESTION

1. What is the difference between vulnerability analysis systems and intrusion detection systems?
2. What are the limitations of IDS(s)?
3. How do you select the best IDS for your organisation?

REFERENCES

Charles P. Pfleeger (2003). *Security in Computing*. New Jersey, United State: Prentice Hall.

Computerworld blogs (2009). *Application control coming your way*. http://blogs.computerworld.com/node/3890

Donald L.Pipkin (2000). *Information Security*. Upper Saddle River, NewJersey: Prentice Hall.

Interloci Network Management (2002). *Network Intrusion Monitoring*. www.interloci.com/download.cfm/Interloci_Network_Intrusion.pdf

Lumension (2009). *Sanctuary Application Control*. http://www.lumension.com/Sanctuary_AC_Endpoint_Security.jsp

SANS Institute (2009). *Intrusion Detection FAQ: What is intrusion detection?* http://www.sans.org/resources/idfaq/what_is_id.php

TechTarget (2009). *Intrusion detection*. http://searchmidmarketsecurity.techtarget.com/sDefinition/0,sid198_gci295031,00.html

Wikipedia (2009). *Vulnerability (computing)*. http://en.wikipedia.org/wiki/Vulnerability_(computing)

Wikipedia (2009). *Information Technology Control*. http://en.wikipedia.org/wiki/Information_technology_controls#IT_Application_Controls