Standards And Practices Necessary To Implement A Successful Security Review Program For Intrusion Management Systems

By
Alpay DORUK

121018

A Dissertation Submitted to the
Graduate School in Partial Fulfillment of the
Requirements for the Degree of

MASTER OF SCIENCE

Department: Computer Engineering
Major: Computer Software

Izmir Institute of Technology
Izmir, Turkey

August, 2002

121018

We approve the thesis of **Alpay DORUK**

Date of Signature

28.08.2002

Asst. Prof. Tuğkan TUĞLULAR
Supervisor
Department of Computer Engineering

28.08.2002

Prof. Dr. Sıtkı AYTAÇ
Department of Computer Engineering

28.08.2002

Prof. Dr. Şaban EREN
Ege University
Department of Computer Engineering

28.08.2002

Prof. Dr. Sıtkı AYTAÇ
Head of Department

ACKNOWLEDGEMENT

I would like to thank many people that have contributed to the development of this work. First, I would like to thank my thesis advisor Asst. Prof. Tuğkan Tuğlular Ph.D. for his guidance during the long process of this thesis. I would also like to thank Assoc. Prof Ahmet Koltuksuz, Ph.D. for his support and his encouragement, that he gave to me about working in the computer security topic.

I would like to thank all my friends for their support. And especially I would like to thank my family, for their support throughout all my educational career and life.

ABSTRACT

Intrusion Management Systems are being used to prevent the information systems from successful intrusions and their consequences. They also have detection features. They try to detect intrusions, which have passed the implemented measures. Also the recovery of the system after a successful intrusion is made by the Intrusion Management Systems. The investigation of the intrusion is made by Intrusion Management Systems also. These functions can be existent in an intrusion management system model, which has a four layers architecture. The layers of the model are *avoidance, assurance, detection and recovery.* At the avoidance layer necessary policies, standards and practices are implemented to prevent the information system from successful intrusions. At the avoidance layer, the effectiveness of implemented measures are measured by some test and reviews. At the detection layer the identification of an intrusion or intrusion attempt is made in the real time. The recovery layer is responsible from restoring the information system after a successful intrusion. It has also functions to investigate the intrusion.

Intrusion Management Systems are used to protect information and computer assets from intrusions. An organization aiming to protect its assets must use such a system. After the implementation of the system, continuous reviews must be conducted in order to ensure the effectiveness of the measures taken. Such a review can achieve its goal by using principles and standards. In this thesis, the principles necessary to implement a successful review program for Intrusion Management Systems have been developed in the guidance of Generally Accepted System Security Principles (GASSP). These example principles are developed for tools of each Intrusion Management System layer. These tools are firewalls for avoidance layer, vulnerability scanners for assurance layer, intrusion detection systems for detection layer and integrity checkers for recovery layer of Intrusion Management Systems.

ÖZ

Nüfuz Yönetim Sistemleri, bilgi sistemlerini başarılı bir nüfuz olma olasılığından ve bunarın sonuçlarından korumak için kullanılmaktadır. Ayrıca böyle bir nüfuzu tespit etmek de bu sistemlerin özelliklerinden biridir. Uygulanan önlemleri geçen nüfuzlar bu sistemlerce tespit edilmeye çalışılmaktadır. Başarılı bir nüfuzdan sonra sistemi iyileştirip eski konumuna getirmek ve mümkün olursa nüfuz ve nüfuz girişimlerini soruşturmak da bu sistemlerin fonksiyonlarından biridir. Bu fonksiyonlar dört katmanlı bir nüfuz yönetim sistemi modelinde bulunabilir. Bu katmanlar, önlem, güvence, tespit ve iyileştirme katmanlarıdır. Önlem katmanında gerekli politika ve standartlar geliştirilip, gerekli çalışmalar yapılarak bilgi sistemleri başarılı nüfuzlardan korunmaktadır. Güvence katmanında ise, uygulanan önlemlerin etkinliği yapılan test ve incelemeler ile ölçülmektedir. Tespit katmanı gerçek zamanda oluşan nüfuz ve nüfuz girişimlerinin saptanmasından sorumludur. İyileştirme katmanı ise başarılı bir nüfuzun sonucunda bilgi sisteminde ve bilginin kendisinde oluşabilecek hasarların düzeltilmesinden ve sistemin eski güvenli konumuna döndürülmesinden sorumludur. Ayrıca nüfuzun soruşturulması da bu katmanda gerçekleştirilir.

Nüfuz Yönetim Sistemleri bilgi ve bilgi teknolojisi değerlerinin korunmasında kullanılmaktadır. Değerlerini korumayı hedefleyen bir organizasyon böyle bir sistem kullanmalıdır. Sistemin gerçekleştirilmesinden sonra ise alınan önlemlerin etkinliğinin garanti edilmesi için devamlı bir inceleme gereklidir. Bu tip bir inceleme hedefine prensip ve standartlar kullanarak ulaşabilir. Bu tezde, Nüfuz Yönetim Sistemleri için başarılı bir güvenlik inceleme programı geliştirmek için gerekli prensipleri Genel Olarak Kabul Edilmiş Sistem Güvenlik Prensipleri'nin yol göstericiliği ortaya konmuştur. Nüfuz Yönetim Sistemleri'nin her katmanından örnek araçlar için prensipler geliştirilmiştir. Bu araçlar; önlem katmanı için güvenlik duvarları, güvence katmanı için zayıflık tarama araçları, tespit katmanı için Nüfuz Tespit Sistemleri ve iyileştirme katmanı için bütünlük kontrolü araçlarıdır.

TABLE OF CONTENTS

TABLE OF FIGURES

CHAPTER 1

INTRODUCTION

Computers and computer systems holds important information and data for people, organizations and enterprises. This information should be protected and stored in a secure environment without giving a chance to be modified, added or deleted by unauthorized persons, users or attackers, which can be named as intruders. The efforts, attacks and misuses of computers or computer systems to obtain classified information, for theft or maybe just for pleasure are called as intrusion.

Some measures should be taken to avoid these intrusion to give harm to the system. Combination of measures against these intrusions are called as Intrusion Management Systems. The primary goal of intrusion management systems is to prevent the consequences of intrusions entirely. Intrusion management is a four-layer process. These four layers are avoidance, assurance, detection and recovery, with a sub-layer investigation.

The first step in Intrusion Management process is avoidance. Avoidance includes all of those underlying processes that seek to create a secure environment. All the intrusions are tried to be prevented in this layer of Intrusion Management Systems. The second step is assurance. Assurance includes everything done to ensure the policies, standards and practices are being followed. Also the vulnerabilities of the system should be checked in this layer. Also some intrusion tests to the information system should be done in this layer. The third step is detection. In this layer the real time detection of an intrusion attempt is very important. Knowing that an attack is in progress and being able to take immediate action improves the chance of successfully terminating an intrusion and the intruder. Real time detection depends upon having an audit system that sits in the background and watches all the activities involving the device under surveillance. The last step is recovery, with a sub-layer investigation. Intrusion management defaults the recovery when al the other steps are failed to prevent the consequences of a successful attack. Recovery requires the construction of the system to the point where it is sure that the system have not been altered by the intruder. The data lost is between the attack and the last backup. Investigation of security incidents, whether they are successful or simply strong attempts, should be examined by the organizations' Computer Incident Response Teams (CIRT). The CIRT should be trained and prepared to initiate a formal investigation, present results to management, support litigation or criminal prosecution if necessary, and ensure that lessons learned are fed back to the Intrusion Management process.

Such a system should also be controlled and its security review should be made. While doing this process some principles, standards and practices can be used. The primary goal of this thesis is to develop some principles, that can be used in implementing such a security review program for Intrusion Management Systems. In this thesis Generally Accepted System Security Principles (GASSP) have been used in order to develop some principles for implementing a successful security review program for Intrusion Management Systems.

The principles developed in this thesis are about *firewalls*; which take place in avoidance layer of Intrusion Management systems, *vulnerability scanners*; which are in assurance level of Intrusion Management Systems, *Intrusion Detection Systems*; which are in detection layer of Intrusion Management Systems and *integrity checkers*; which are in recovery layer of Intrusion Management Systems. Principles developed in this thesis can be used by organizations' security administrators in security review job of their Intrusion Management Systems.

The Chapters of the thesis are formed as follows. In the second chapter of this thesis, a background and overview about computer misuse techniques, Intrusion Management Systems and finally about Generally Accepted System Security Principles is given. In Chapter 3, the usage of GASSP principles in the implementation of security review process are explained and new principles are developed. Also some examples of tools have been explained and their qualifications are listed. In Chapter 4 a conclusion about the principles have been made. Also a glossary for some terms used is included in the appendix of the thesis.

CHAPTER 2

BACKGROUND AND OVERVIEW

In this chapter, an overview about techniques of computer misuses, Intrusion Management Systems and finally about Generally Accepted System Security Principles is presented.

2.1 Computer Misuse Techniques

Computer misuse can be described as, "The willful or negligent unauthorized activity that affects the availability, confidentiality, or integrity of computer resources. Computer abuse includes fraud, embezzlement, theft, malicious damage, unauthorized use, denial of service, and misappropriation." [1]. There are three types of basic gaps that computer misuses can exploit [2]:

- "The technological gap between what a computer system is actually capable of enforcing and what is expected to enforce (policies) This gap includes deficiencies in both hardware and software as well as their administration, configuration and operation."
- "The sociotechnical gap between computer policies and social policies, such as computer related crime laws, privacy laws and codes of ethics. When the computer policies are not consistent with the socially expected norms this kind of gap can arise."
- "The social gap between social policies and actual human behavior. This gap arises when people do not act according to expectations."

The attackers use these gaps in committing computer misuses. There are several types of computer misuses techniques. We can group them in different classes. These techniques can be classified as follows [2]:

- External Misuse - This class of misuse is generally non-technical and unobserved and generally computers are not used in this type of misuses. If we should give an example to this technique; collection of waste papers, remote observation of typed keystrokes can be given. These techniques have no direct effects on the computer systems and cannot be detected by the computer security systems, but data that can be captured by these means can be used in implementing other technological attacks.

- Hardware Misuse - There are two types of hardware misuse techniques. Passive and active hardware misuse:
  - Passive hardware misuse techniques have no immediate side effects on hardware or software behavior. For example, eavesdropping and logical scavenging.
  - Active hardware misuses have direct effects on computer systems. This type of misuse includes computing equipment and storage media theft, hardware modifications and physical attacks.

- Masquerading - These activities may be indistinguishable from legitimate activity. Impersonation, playback and spoofing attacks, piggybacking on other users can be examples of this type of attacks

- Setting up subsequent misuse - This class of misuses is planting and arming the software Trojan horses with techniques of such as logic bombs, time bombs, malicious worms and viruses. These programs may actually employ misuses of other classes such as bypasses or misuse of authority.

- Bypassing intended controls - This class of misuse is circumvention of existing controls or improper acquisition of otherwise denied authority, presumably with the intent to subsequently misuse the acquired access rights.

- Active misuse of resources - This class of misuse is misuse of conferred authority that alters the system or its data. For example, misuse of administrator privileges or superuser privileges.

- Passive misuse of resources - This class includes misuse of conferred reading authority, such as browsing (without specific target), searching (for specific patterns), access to data aggregates that are more sensitive than the individual items and exploitation of covert channels.

- Misuse resulting from inaction - This class of misuse is a failure to avert a potential problem in a timely fashion, or an error of omission, for example. This class might be considered as a limiting case of passive misuse; however, it seems qualitatively different and thus is distinguished as a separate class. Intentional misuse would result from someone detecting but not reporting a serious security flaw.

- Use as an aid to other misuses - This class has two kinds;
  - ♦ As a tool in planning, developing, controlling, or carrying out computer-system misuse, such as seeking matches in the encrypted password file by preencrypting dictionaries and likely passwords. Activities of this subclass may subsequently lead to other computer misuse classes. This activities could be aimed at attacking a computer system other than the one on which the indirect misuse is carried out. This activities may seem suspicious, but is not necessarily yet an overt abuse.
  - ♦ As a tool in planning, developing, controlling, or engaging in criminal enterprise (e.g., managing an illegal drug business, or committing financial fraud), or performing unethical acts (e.g., misuse of company resources for private purposes).

Also a distinction between *abuse* and *misuse* must be made, using abuse to refer to intentional acts, and misuse to refer more generally to accidental or intentional act. The classification addresses both intentional abuses of computers and corresponding accidental misuses, primarily from the vantage point of security; however, we note that there are other accidental forms of misuse that are not represented here.

One person can do most of the abuses above, but also there are misuses that many people collaborate in omitting them. This type of misuses can be named as *collaborative misuses.* And if the target computer system uses compartmentation and multi-person authorizations collaborative misuses can be a necessity. For example successful Trojan horses may require the unwitting collaboration of victims, but the abuse by only one person.

2.2 Intrusion Management Systems

Intrusion can be described as, "Any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource" [1]. As the scale of networks grows, the protection of assets from compromise, misuse, damage or destruction become harder and harder. So a new model of information protection must be developed, because the traditional protection measures, such as access controls, became insufficient to protect the assets. The objectives of such an Information Protection Model can be stated as stated below [3]:

An acceptable information protection model should accomplish three broad goals [3]:

- It should accommodate mechanisms that protect information assets from compromise, abuse, damage or destruction.
- It should recognize that compromise is inevitable and that measures must be taken in advance of to compromise to facilitate a means for recovery.
- The model should provide feedback that can speed response to a compromise and generate information that can be used to prevent similar compromises in the future. It is implicit in such a model that recovery is of greater urgency than prosecution.

The requirements of this kind of model are [3]:

- Information security architecture should strive to protect information assets from compromise, abuse, destruction or damage. This is the primary objective of information security in general.
- Some form of quality assurance must be present to verify that the actions taken by components of the first requirement were effective and sufficient to the overall task.
- The model must take into account that intrusion attempts would occur and that some percentage, depending upon the effectiveness of the implementations of the first two requirements, would succeed. The model must provide for the detection attempt and forensic collection and management of appropriate evidence.
- Proceeding from the third requirement, the organization must be in a position to pursue the investigation of intrusion attempts and act upon the evidence in accordance their local policies. Because investigative motives differ (pursuing the perpetrator,

recovering from the attack, responding to insurance requirements are just a few) the requirements for the investigation layer may differ from instance to instance.

In addition to the four basic requirements, there must be a system of feedback loops that allow the various capabilities of an architecture implemented under the model interact. The resulting model, stated as *Intrusion Management*, has the following stated purpose [4]:

> "Limiting the possibility of a successful intrusion through effective
> preventive, quality management and detective processes, and
> facilitating successful investigation of an intrusion or an intrusion
> attempt should either occur."

This goal can be addressed by implementing effective security controls. These controls must aim the vulnerabilities of the system. There are six functional areas of vulnerability. These are [4]:

- Identification and Authentication: Functions intended to establish and verify the identity of the user or using process.
- Access Control: Functions intended to control the flow of data between, and the use of resources by users, processes and objects. This includes administration and verification of access rights.
- Accountability: Functions intended to record exercising of rights to perform security-relevant actions.
- Object Reuse: Functions intended to control reuse or scavenging of data objects.
- Accuracy: Functions intended to insure correctness and consistency of security-relevant information.
- Reliability of Service: Functions intended to insure security of data over communication links.

To address the goal of preventing intrusions, an intrusion management system should have a four layer architecture. These layers are [3]:

- Avoidance Layer
- Assurance Layer
- Detection Layer

- Recovery Layer (with the Investigation Sublayer)

2.2.1 Layers of Intrusion Management Systems

The Intrusion Management model consists of four layers one sublayer and feedback loops. The feedback loops provide action mechanisms between the various levels of the model. For example, an Intrusion Detection System (IDS) implemented in layer 3 (Detection) has a feedback loop to layer 1 (Avoidance) which allows for notification that an event is occurring and triggers the appropriate response to avoid the consequences of the event. An IDS that did not implement such a feedback loop would not meet the requirements of the model. The four layers of the model are defined as follows [3]:

2.2.1.1 Layer 1 - Avoidance

The first step in Intrusion Management process is **avoidance**. Avoidance is defined as all of those underlying processes implemented to create a secure environment. Those processes may be administrative, as in policies, standards and practices, or they may be technological as in the application of access control tools. Some examples of Avoidance are [3]:

- Security policy
- Standards and practices
- Security Awareness
- Incident response planning
- Disaster planning
- Training of security and IT Audit personnel
- Evaluating the results of a successful intrusion (" lessons learned" feedback)
- Implementation of access control programs
- Implementation of firewalls
- Implementation of encryption

2.2.1.2 Layer 2 – Assurance

The second step is **assurance**. Assurance is defined as everything done to ensure that policies, standards, practices and technological controls are effective. These processes include [3]:

- IT audits
- Intrusion or penetration testing
- Vulnerability assessments
- Security reviews

Using appropriate tools, we can test our systems for vulnerabilities and, through proper configuration or use of third party products, we can ensure that appropriate steps are taken to reduce or eliminate them. Tools that we should use are of two types: preventative and detective.

Preventative tools include those that we use to perform initial evaluation and configuration. Detective tools are intended to ensure that any change of the configuration is detected.

2.2.1.3 Layer 3 – Detection

The third step is **detection**. "Detection, as used here, is somewhat different from the detective controls present during the avoidance and testing steps. In this case Detection is defined as measures used to detect an intrusion or abuse attempt in real time. The real time aspect of detection is important: knowing that an attack is in progress and being able to take immediate action greatly improves the odds of successfully terminating the intrusion and apprehending the perpetrator" [3].

Real time detection depends upon having a "watch dog" system that sits in the background and watches all activities involving the device under surveillance. The watch dog also must be able to interpret what constitutes an attack. The watch dog should be able to detect abuse attempts both on communications channels and at the device itself. It should comprise both network and device based surveillance.

Critical components of the Detection level are the ability to collect forensically pristine data that will help us to investigate and prosecute the perpetrator of an intrusion or intrusion attempt, the ability to preserve that data from alteration and the ability to trigger appropriate response actions.

2.2.1.4 Layer 4 - Recovery and Investigation

The fourth step is **recovery**. "Intrusion Management defaults to Recovery when all other measures have failed to prevent the consequences of a successful attack. After the recovery layer, there is an investigation sub-layer, in this sub-layer the traces of the intrusion are investigated and the intruder is tried to be catch." [3]

2.2.1.4.1 Recovery Layer

Recovery requires that we reconstruct the victim machine to the point where we can state with confidence that we are not encroaching on information (configuration or otherwise) that may have been altered by the intruder. Often this means losing data that was generated in the "delta" between the time of the attack and the time of the last valid backup. For this reason we may move into the sub-layer of Investigation in order to use forensic techniques to recover the system.

2.2.1.4.2 Sublayer – Investigation

If it is the intent of the system owner to pursue a formal investigation aimed at identifying the perpetrator of an attack, the Investigation sub-layer of recovery comes into play. However, investigation, as you may have already gathered, may be futile unless luck and circumstances are with you. By integrating your investigation process into the intrusion management methodology you improve your odds markedly because you have gathered significant important information and made critical preparations along the way.

The Investigation sub-layer is defined as those processes used to determine the source and nature of an intrusion or abuse attempt, to gather, preserve and manage evidence relating to the attempt, and to institute appropriate action as defined by local policy.

2.2.1.5 Feedback and Service Loops

The concept of feedback and service loops is one of the distinguishing factors of the Intrusion Management model. This concept recognizes that the individual layers of the Model do not operate in isolation. Feedback loops offer a method of providing information from one layer to a lower layer, while service loops provide services from one layer to a higher layer. For example there is an important feedback loop to layer 1 (Avoidance) from layer 4 (Recovery). This feedback loop consists of lessons learned in the investigation of an abuse attempt. Presumably, those lessons will contribute to avoiding the consequences of a similar attack later.

There are, of course, other feedback and service loops within the Model. Some of these involve Layer 3 (Detection). There is a service loop from Assurance to Detection. When we perform vulnerability assessments, we use intrusion detection systems to monitor our tests. We can extend that service loop from Detection to the Investigation sub-layer. The patterns recognized by our intrusion detection system are important in interpreting logs in an incident investigation.

A feedback loop exists between Avoidance to Detection. When an intrusion detection system (more correctly, intrusion detection and response system) detects an abuse attempt, it has, depending upon local policy, several response options. One of those options may be to terminate the socket. Terminating a socket with an intruder is, clearly, an avoidance measure.

2.3 Generally Accepted System Security Principles (GASSP)

Formation of the I^{2}SF-sponsored GASSP Committee (GASSPC) began in mid-1992 in response to Recommendation #1 of the report "Computers at Risk" (CAR), published by the United States of America's National Research Council in 1990. That recommendation, "To Promulgate Comprehensive Generally Accepted System Security Principles," and its subordinate elements sparked the genesis of a concerted effort to establish a well-balanced committee population representing key elements of the private and public sectors from both the USA and abroad.

Both administrative and product-related principles are being addressed, individual and organizational privacy rights are being addressed, and, to consolidate all the elements of a rapidly evolving industry, alliances are being established to the International Information Systems Security Certification Consortium (ISC)^2, the international Common Criteria effort to develop information technology product-related information security principles, and other organizations having an interest in the security of information and associated principles.

In order to effectively consolidate and sustain the value of comprehensive GASSP, the CAR recommendation envisions the creation of an authoritative infrastructure to maintain the GASSP, support their evolution, enforce "compliance", and provide a vehicle for the authoritative approval of reasonably founded exceptions or departures from GASSP. This authoritative infrastructure would be modeled after those that support and sustain the Generally Accepted Accounting Principles (GAAP) and like models of the international accounting profession.

The GASSP Committee kickoff meeting was held at the 1992 National Computer Security Conference in Baltimore, Maryland, USA, and was attended by twenty-five leading information security experts from the USA, Canada, the UK, France, Germany, the Netherlands, Sweden, and the European Commission (EC). Many differing perspectives and agendas were discussed in an open exchange, but at the close of the meeting, it was the consensus that the objectives were important, necessary, and, perhaps most significant, achievable.

2.3.1 Definition

Information security is a combination of preventive, detective, and recovery measures. A preventive measure is a risk control that avoids or deters the occurrence of an undesirable event. Passwords, keycards, badges, contingency plans, policies, firewalls, and encryption are examples of preventive measures. A detective measure is a risk control that identifies the occurrence of an undesirable event. Visitor logs, audit trails, motion sensors, closed circuit TV, and security reviews are examples of detective controls. Detective measures also provide a means for reporting the occurrence of events. A recovery measure is a risk control that restores the integrity, availability, and confidentiality of information assets to their expected state. Examples of recovery measures are fault tolerance, backup, and disaster recovery plans.

Information Security also includes education, awareness, and training measures that inform computer users of the “acceptable use” principles and practices that support the protection of information assets. The introduction of GASSP supports and strengthens these controls. These principles should be constructed to ensure that the information system reduces the possibility of a risk event and its impact.

2.3.2 Purpose, Scope and Objectives

The GASSP Committee seeks to develop and maintain GASSP with guidance from information owners, information security practitioners, information technology product developers, and organizations having extensive experience in defining and stating the principles of information security. The GASSP Committee seeks the creation, maintenance, monitoring of, and adherence to the GASSP for information security in the broadest context, on an international level, unifying and expanding upon existing authoritative sources [5].

The objectives of GASSP Committee in forming the Generally Accepted System Security Principles are [5]:

- “Identify and develop Pervasive, Broad Functional, and Detailed GASSP and protection profiles in a comprehensive framework of emergent principles, standards, conventions, and mechanisms that will preserve the availability, confidentiality, and integrity of information.”

- "Be an authoritative source for opinions, practices, and principles for information owners, information security practitioners, information technology products, and information systems."

- "Define, implement, and subsequently operate under the governing GASSP infrastructure."

- "Define and establish linkage to the Common Criteria Project."

- "Maintain close liaison and coordination with other international authoritative bodies that have developed related works, to establish and maintain GASSP based on these efforts."

- "Define and establish liaison with bodies responsible for certifying professionals to encourage convergence."

- "Promote broad awareness of information security and GASSP."

- "GASSP will address management, user, and other interested parties' concerns at all levels to gain the broadest acceptance."

2.3.3 Principles

There are three kinds of Generally Accepted System security Principles and they are organized in a three-level hierarchy. The hierarchy is comprised of Pervasive Principles (PP), Broad Functional Principles (BFP) and Detailed Security Principles (DSP). The hierarchy goes from the fundamental one to detailed one.

2.3.3.1 Pervasive Principles

Pervasive principles are few in number, fundamental in nature, and rarely changing. The Pervasive Principles address the following properties of information [5]:

- Confidentiality
- Integrity
- Availability

The Pervasive Principles provide general guidance to establish and maintain the security of information. These principles form the basis of Broad Functional Principles and Detailed Principles. Security of information is achieved through the preservation of appropriate confidentiality, integrity, and availability. Confidentiality is the characteristic of information being disclosed only to authorized persons, entities, and processes at authorized times and in the authorized manner. Integrity is the characteristic of information being accurate and complete and the information systems' preservation of accuracy and completeness. Availability is the characteristic of information and supporting information systems being accessible and usable on a timely basis in the required manner.

The Pervasive Principles are founded on the Guidelines for Security of Information Systems, developed by the Information Computer and Communications Policy (ICCP) Committee and endorsed and published by the Organization for Economic Cooperation and Development (OECD).

The OECD principles have been interpreted and extended using the Authoritative Foundation, a list of fundamental works on information security compiled by the GASSP Committee to support the development of GASSP.

The list and explanations of pervasive principles are as follows [5]:

- **Accountability Principle (PP-1)** - The GASSP statement for this principle is stated as, "Information security accountability and responsibility must be clearly defined and acknowledged."[5] Accountability characterizes the ability to audit the actions of all parties and processes, which interact with information. Roles and responsibilities are clearly defined, identified, and authorized at a level commensurate with the sensitivity and criticality of information. The relationship between all parties, processes, and information must be clearly defined, documented, and acknowledged by all parties. All parties must have responsibilities for which they are held accountable.

- **Awareness Principle (PP-2)** - The GASSP statement for this principle is stated as, "All parties, including but not limited to information owners and information security practitioners, with a need to know should have access to applied or available principles, standards, conventions, or mechanisms for the security of information and information systems, and should be informed of applicable threats to the security of information." [5] This principle applies between and within organizations. Awareness of information security principles, standards, conventions, and mechanisms enhances and enables controls and can help to mitigate threats. Awareness of threats and their significance also increases user acceptance of controls. Without user awareness of the necessity for particular controls, the users can pose a risk to information by ignoring, bypassing, or overcoming existing control mechanisms. The awareness principle applies to unauthorized and authorized parties.

- **Ethics Principle (PP-3)** - The GASSP statement for this principle is stated as, "Information should be used, and the administration of information security should be executed in an ethical manner." [5] Information systems pervade our societies and cultures. Rules and expectations are evolving with regard to the appropriate provision and use of information systems and the security of information. Use of information and information systems should match the expectations established by social norms, and obligations.

- **Multidisciplinary Principle (PP-4)** -The GASSP statement for this principle is stated as, "Principles, standards, conventions, and mechanisms for the security of information and information systems should address the considerations and viewpoints of all interested parties." [5] Information security is achieved by the combined efforts of information owners, users, custodians, and information security personnel. Decisions made with due consideration of all relevant viewpoints and technical capabilities can enhance information security and receive better acceptance.

- **Proportionality Principle (PP-5)** - The GASSP statement for this principle is stated as, "Information security controls should be proportionate to the risks of modification, denial of use, or disclosure of the information." [5] Security controls should be commensurate with the value of the information assets and the vulnerability. Consider the value, sensitivity and criticality of the information, and the probability, frequency and severity of direct and indirect harm or loss. This principle recognizes the value of approaches to information security ranging from prevention to acceptance.

- **Integration Principle (PP-6)** - The GASSP statement for this principle is stated as, "Principles, standards, conventions, and mechanisms for the security of information should be coordinated and integrated with each other and with the organization's policies and procedures to create and maintain security throughout an information system." [5] Many breaches of information security involve the compromise of more than one safeguard. The most effective control measures are components of an integrated system of controls. Information security is most efficient when planned, managed and coordinated throughout the organization's system of controls and the life of the information.

- **Timeliness Principle (PP-7)** - The GASSP statement for this principle is stated as, "All accountable parties should act in a timely, coordinated manner to prevent or respond to breaches of and threats to the security of information and information systems." [5] Organizations should be capable of swift coordination and action to enable threat event prevention or mitigation. This principle recognizes the need for the public and private sectors to jointly establish mechanisms and procedures for rapid and effective threat event reporting and handling. Access to threat event history could support effective response to threat events and may help to prevent future incidents.

- **Assessment Principle (PP-8)** - The GASSP statement for this principle is stated as, "The risks to information and information systems should be assessed periodically." [5] Information and the requirements for its security vary over time. Risks to the information; its value; and the probability, frequency, and severity of direct and indirect harm/loss should undergo periodic assessment. Periodic assessment identifies and measures the variances from available and established security measures and controls, such as those articulated here in the GASSP, and the risk associated with such variances. Periodic assessment enables accountable parties to make informed, information risk management decisions whether to accept, mitigate, or transfer the identified risks with due consideration of cost effectiveness.

- **Equity Principle (PP-9)** - The GASSP statement for this principle is stated as, "Management shall respect the rights and dignity of individuals when setting policy and when selecting, implementing, and enforcing security measures." [5] Information security measures implemented by an organization should not infringe upon the obligations, rights, and needs of legitimate users, owners, and others affected by the information when exercised within the legitimate parameters of the mission objectives.

2.3.3.2 Broad Functional Principles

Broad Functional Principles are subordinate to one or more of the Pervasive Principles, are more numerous and specific, guide the development of more Detailed Principles, and change only when reflecting major developments in technology or other affecting issues.

The Broad Functional Principles (BFPs) are derived from the Pervasive Principles (PP) that represent the conceptual goals of information security. By providing the guidance for operational accomplishment of the Pervasive Principles, the Broad Functional Principles are the building blocks (what to do) that comprise the Pervasive Principles and allow definition of the basic units of those principles. Because the Broad Functional Principles are smaller in scope, they are easier to address in terms of implementation planning and execution.

The list and explanations of broad functional principles are as follows [5]:

- **Information Security Policy (BFP-1)** - The GASSP statement for this principle is stated as, "Management shall ensure that policy and supporting standards, baselines, procedures, and guidelines are developed and maintained to address all aspects of information security. Such guidance must assign responsibility, the level of discretion, and how much risk each individual or organizational entity is authorized to assume." [5] In order to assure that Information assets are effectively and uniformly secured consistent with their value and associated risk factors, management must clearly articulate its security strategy and associated expectations. In the absence of this clarity, some resources will be under-secured - that is, ineffective; other resources will be over-secured - that is, inefficient.

- **Education and Awareness (BFP-2)** - The GASSP statement for this principle is stated as, "Management shall communicate information security policy to all personnel and ensure that all are appropriately aware. Education shall include standards, baselines, procedures, guidelines, responsibilities, related enforcement measures, and consequences of failure to comply." [5] In order to ensure that all personnel are effectively aware of security policy, management must effectively and regularly communicate its requirements. When personnel fail to do what management expects, it is more often the result of an ineffective or imperfect communication of what management expects, rather than from the result of wrongful motive or intent on the part of the personnel. The failure to regularly and effectively communicate information security policy, standards, baselines, procedures, guidelines, responsibilities, related enforcement measures, and the consequences of failing to comply, to all relevant parties can cause the unintentional breach of policy by parties to whom the policy has not been effectively communicated. Such failure can also result in the intentional breach of policy by parties to whom the adverse consequences of such a breach have not been effectively communicated. In both cases, the potential for harm, liability, or loss to the organization or other relevant parties can be significant. The failure to effectively communicate information security policy can also impair the ability to successfully apply enforcement measures, prosecute criminal activity, or seek civil redress.

- **Accountability (BFP-3)** - The GASSP statement for this principle is stated as, "Management shall hold all parties accountable for their access to and use of information, e.g., additions, modifications, copying and deletions, and supporting Information Technology resources. It must be possible to affix the date, time, and responsibility, to the level of an individual, for all significant events." [5] In order to assure that people behave as expected, it is necessary to know who did what and when it was done. It is essential that organizations establish and maintain a basis of control for information assets. Such a control framework requires individual and organizational accountability at all levels. The concept of "accountability" refers to the accepting of responsibility by all relevant parties or entities. Holding all parties accountable is intended to assure that any use made of or actions taken on information assets and supporting Information Technology resources shall be for authorized "business/mission purposes only" and that such use or action can be reliably traced to the responsible party or parties, who will be held "accountable."

• **Information Management (BFP-4)** - The GASSP statement for this principle is stated as, "Management shall routinely catalog and value information assets, and assign levels of sensitivity and criticality. Information, as an asset, must be uniquely identified and responsibility for it assigned."[5] In order to manage information assets efficiently, management must know what to protect. In order to be effectively managed, it is essential to identify and enumerate the core attributes of information as assets. The organizational ownership of an information asset must be established. The person or agent/custodian legitimately established as the owner of an information asset has the authority and responsibility to make - or delegate - decisions regarding the security of the information asset. It is typically the organization that will ultimately suffer liability, loss, or other harm if the confidentiality, availability, or integrity of the information asset is compromised, though others may suffer harm or loss as well. The identity and content of the information asset must be clearly established for the owner to make informed decisions regarding its security. Knowing the value of the information asset, as related to its confidentiality, availability, and integrity, enables the owner to understand the financial risks and associated threats that must be mitigated when establishing security requirements for the information asset. Finally, these attributes should be reviewed regularly, because most information attributes change value over time - in some cases increasing and in others, decreasing.

• **Environmental Management (BFP-5)** - The GASSP statement for this principle is stated as, "Management shall consider and compensate for the risks inherent to the internal and external physical environment where information assets and supporting Information Technology resources and assets are stored, transmitted, or used." [5] In order to effectively protect the organizational mission, it is necessary to identify and address environmental threats that can disrupt Information Technology functionality. There are significant threats - and vulnerabilities - associated with the location, construction, and equipping of Information Technology facilities. These threats include: Natural disaster threats (earthquake, flood, hurricane, tornado, landslides, etc.), and unintentional or intentional physical threats (e.g., power outage, equipment failure, fire, proximity of potentially toxic or explosive industrial facilities and transportation infrastructures, local crime, and a wide array of accidents that could "exploit" unrecognized or inadequately addressed vulnerabilities of the physical environment.). For the optimum security strategy implementation, it is essential to coordinate and integrate information security efforts with overall organizational security measures and management. Failure to recognize and effectively address local threats and associated vulnerabilities, both internal and external, can result in a potentially disastrous disruption of Information Technology functionality.

- **Personnel Qualifications (BFP-6)** - The GASSP statement for this principle is stated as, "Management shall establish and verify the qualifications related to integrity, need-to- know, and technical competence of all parties provided access to information assets or supporting Information Technology resources." [5] In order to effectively implement security for information assets and supporting Information Technology resources, it is necessary that the personnel involved are competent with respect to the knowledge and technical skill needed to perform their roles reliably, that their integrity (as demonstrated by work history, academic and training certification, and references) meets organizational requirements, and that their need-to-know is authoritatively established

- **System Integrity (BFP-7)** - The GASSP statement for this principle is stated as, "Management shall ensure that all properties of systems and applications that are essential to or relied upon to support the organization's mission are established, preserved, and safeguarded." [4] In order for Management to be able to rely upon the correct performance of Information Technology resources, it is necessary to ensure that they are implemented as intended and are not subsequently contaminated or corrupted by malicious acts, uncorrected error conditions, or other failures. Unless controls are in place to protect systems and applications from unauthorized modifications and to ensure that authorized changes are tracked and perform as intended, systems can fail in a way that impairs efficiency or even the health of the organization. Further, such failures may not be detected on a timely basis, because management assumes the integrity of the Information Technology resources.

- **Information Systems Life Cycle (BFP-8)** - The GASSP statement for this principle is stated as, "Management shall ensure that security is addressed at all stages of the system life cycle." [5] In order for management to be able to rely upon controls, they must be continuous. In order to be efficient, controls must be comprehensive and applied early. The security function must be fully integrated with system life cycle processes. Retrofit, repair, and other late remedies are always inefficient and may be ineffective. Late application of a control may be insufficient to restore a system to a desired or required robustness. All in-place controls and countermeasures must be fully documented and periodically reviewed. For pre-production systems, phase reviews must assess intended security feature design, integration, and effectiveness. For in-production systems, maintenance phase reviews must be performed at every step to ensure consistent and correct performance, continued effectiveness and efficiency, accurate interface(s) with other applications, and the comprehensive maintenance of all contingency planning measures. All reviews must be conducted in conformance with established guidelines that define minimum acceptable requirements for controls' effectiveness in support of organizational standards for information confidentiality, system and data integrity, and the availability of the information asset and supporting Information Technology resources.

- **Access Control (BFP-9)** - The GASSP statement for this principle is stated as, "Management shall establish appropriate controls to balance access to information assets and supporting Information Technology resources against the risk." [5] In order to achieve a level of risk mitigation commensurate with the value of the information asset to be secured, access to information assets and supporting Information Technology resources should be restricted to the smallest population consistent with other business needs, based on the criteria of a clearly delineated "need-to-know." Through this standard, the information systems-dependent workforce is facilitated in the accomplishment of assigned tasks by ensuring that all required information is available only through appropriately controlled means. Specifically, individual employees and other parties are restricted from access to information assets and supporting Information Technology resources that do not directly relate to their work requirements, assigned objectives, or legitimate, authorized need. By enforcing such a standard, the owner or custodian limits the exposure of potentially sensitive information assets and supporting Information Technology resources and enables management to assert appropriate control over the access to, modification of, or the dissemination of sensitive information assets in terms of content and recipient. Therefore, potentially adverse consequences resulting from uncontrolled access or distribution are minimized.

- **Operational Continuity and Contingency Planning (BFP-10)** - The GASSP statement for this principle is stated as, "Management shall plan for and operate Information Technology in such a way as to preserve the continuity of organizational operations." [5] In order to protect information assets and supporting Information Technology resources from disruptive events, or to be able to rapidly restore their proper functioning in the case that such a disruptive event is unavoidable, it is essential that organizations establish a cohesive set of preventive, mitigative, and restorative measures, as determined to be appropriate and cost-effective by risk assessment. Organizational entities depend on their Information Technology resource infrastructure now more than at any previous time in history to deliver mission-critical information in a timely fashion. The operational importance of information assets, whether based on cost or time factors, is such that organizations can ill afford to endure the consequences of significantly disruptive events impacting supporting Information Technology resources or the information assets directly.

- **Information Risk Management (BFP-11)** - The GASSP statement for this principle is stated as, "Management shall ensure that information security measures are appropriate to the value of the assets and the threats to which they are vulnerable." [5] In order to choose effective and efficient information security measures, management must identify the assets to be protected, the threats to the assets, and the vulnerability of the assets or their environment to the threats. Well-informed owners, managers, custodians, or other responsible parties must assure the security of information assets, with regard to the value of their confidentiality, integrity, and availability, and the security of the supporting Information Technology resources. Such an approach (performed strategically, on an on-going basis, or as changes dictate) must enable well-informed decisions regarding whether to accept, mitigate, or transfer the risks associated with the information assets and supporting Information Technology resources. These decisions should be based on the monetary value of the assets, probability and consequences of direct or indirect harm or loss, related threats, effectiveness of existing safeguards and controls, and whether additional safeguards oı controls could be expected to provide cost-effective incremental risk mitigation.

• **Network and Infrastructure Security (BFP-12)** - The GASSP statement for this principle is stated as, "Management shall consider the potential impact on the shared global infrastructure, e.g., the Internet, public switched networks, and other connected systems when establishing network security measures." [5] In order to compensate for the increased vulnerability from and to things outside of the organization, as created by connection to systems beyond the organization, the threat and risk model must be changed to reflect the threat from and to things outside the organization. For example, connecting a UNIX system to the public switched network puts the UNIX system at risk, and connecting the UNIX system to the Internet puts other systems at risk. All methods for accessing Information Technology resource connectivity must contain controls and counter-measures that implement the established security policy of the organization appropriate to the sensitivity or criticality level of the Information Technology resources and supported information assets. Such controls must, at a minimum, reflect the same security level as the information itself to ensure consistency and cohesiveness of overall policy implementation. This consideration must extend to the physical as well as the logical aspect of the connectivity. The potential to subvert access to the Information Technology resources and supported information assets is greatest in terms of connectivity through persistent connections, but increases with temporary connections. This same potential exists, however, through in-house networks, though these are inherently less flexible in their vulnerability to exploitation. Therefore, the security implementation must first identify the specific weaknesses in each access method and the potential consequences of their exploitation. Then each weakness can be addressed through the application of measures intended to achieve a level of protection commensurate with the sensitivity/criticality of the Information Technology resource and the supported information assets.

- **Legal, Regulatory, and Contractual Requirements of Information Security (BFP-13)** - The GASSP statement for this principle is stated as, "Management shall take steps to be aware of and address all legal, regulatory, and contractual requirements pertaining to information assets." [5] In order for an organization to diligently comply with all legal, regulatory, and contractual requirements associated with its operations, it is necessary to ensure that no requirement exists for which compliance measures have not been put in place. As part of this effort, plans should also be in place to address potential actions against the organization should their policy, processes, or actions be called into question.

- **Ethical Practices (BFP-14)** - The GASSP statement for this principle is stated as, "Management shall respect the rights and dignity of individuals when setting policy and when selecting, implementing, and enforcing security measures." [5] In order to preserve employee morale and the perception of the organization and its management as fair and ethical, and recognizing that security measures may be or become unduly intrusive, management must be candid, fair, and conservative in developing and enforcing security policy. Management must carefully consider employee privacy. The key to successful policy is strict observance of fairness and respect for the individual. No policy is complete proof against culpability, but careful construction and consistently unbiased execution contribute positively to the organization's overall risk management program. Policy provisions, including consequences for non-compliance, must be understandable and enforceable, and enforcement must be fairly applied. Candor helps ensure fairness. Security measures that cannot be disclosed should not be applied.

The following matrix in Figure 2.1 presents the relationship of Broad Functional Principles (BFP) to Pervasive Principles (PP). It shows that which pervasive principle is used in developing broad functional principles. For example, while developing Information Management Broad Functional Principle (BFP-4) the pervasive principles;

accountability principle (PP-1), awareness principle (PP-2), multidisciplinary principle (PP-4) and assessment principle (PP-8) are used.

	PP-1	PP-2	PP-3	PP-4	PP-5	PP-6	PP-7	PP-8	PP-9
BFP-1	X	X	X	X	X	X	X	X	X
BFP-2	X	X	X	X					X
BFP-3	X	X	X	X					X
BFP-4	X	X		X				X	
BFP-5	X	X	X	X	X			X	
BFP-6	X	X		X					X
BFP-7	X			X	X	X	X	X	
BFP-8	X			X	X	X	X	X	
BFP-9	X			X	X	X	X	X	
BFP-10	X			X	X	X		X	
BFP-11	X	X		X	X	X	X	X	
BFP-12	X			X	X		X	X	
BFP-13	X	X	X	X					X
BFP-14		X	X	X					X

Figure 2.1: Cross-Impact Matrix Relating BFP's to PP's. [5]

2.2.3.3 Detailed Security Principles

Detailed Security Principles (DSP) are subordinate to one or more of the Broad Functional Principles, are numerous, specific, emergent and change frequently as technology and other affecting issues evolve.

The Detailed Security Principles specifically address methods of achieving compliance with the Broad Functional Principles with respect to existing environments and available technology. There will be many detailed information security principles supporting one or more Broad Functional Principles. The Detailed Principles will address differing technologies, environments, standards, practices, and concepts that are relevant to the Broad Functional Principles. The Detailed Principles are expected to continuously evolve to meet the challenges of emerging technology and new threats.

Following is an example of a Detailed Principle (and its underlying rationale) supporting a Broad Functional Principle (Access Control), which supports the Pervasive Principle (Proportionality) [5]:

- Principle

"Use one-time passwords to control logical access to all information assets deemed critical to an organization."

- Rationale

"Multiple-use passwords were originally the only technique available to control access to a system. Changes in technology made the multiple-use password obsolete in many environments. Therefore, the one-time password evolved. Future technological advances will probably result in the use of smart card technology, replacing current password technology. (There will be separate Detailed Principles that expand upon and guide the application security mechanisms in the users' environment.)"

Also the detailed principles that are developed in this Thesis work about firewalls, vulnerability scanners, intrusion detection systems and integrity checkers can be found on chapter 3.

CHAPTER 3

DEVELOPED GASSP PRINCIPLES IN IMPLEMENTING A SECURITY REVIEW PROGRAM FOR INTRUSION MANAGEMENT SYSTEMS

In this chapter, the usage of GASSP principles for a security review for intrusion management systems with different tools, which take place in different layers; will be explained. These tools are firewalls for avoidance, vulnerability scanners for assurance, intrusion detection systems for detection and integrity checkers for recovery layer.

3.1 Firewalls

Firewalls can be used in avoidance layer of intrusion management systems, and while using and developing such firewalls GASSP principles can be used and GASSP detailed security principle about firewalls can be developed.

A firewall is a protection device used as a filter between a local network and another insecure one. The goals of the firewall are [6]:

- "To check and protect local network hosts from unauthorized disclosing of sensitive information, virus and Trojan Horse attacks,"
- "To protect Internet servers against dangerous commands associated to services ("telnet" or "sendmail") and modifying or deleting files that are vital to the system."

Techniques used for secure Internet gateways are packet filtering, and application-layer proxy. A Packet is used to transfer information across a network and to allow many systems to share it. The information has to be broken into pieces, which are called packets. A packet is a block of data that carries with it the information necessary to deliver it. Packet filtering is a mechanism that control, what data can flow to and from a network. There are no content-based decisions. It is based on source address, destination address, and session and application protocols used. It allows for example; not letting anybody use Telnet to log in from outside or letting everybody send email via SMTP. It won't allow for example, a user can use Telnet in from outside and no other can do so or a user can transfer this file but not those files.

The most common forms of packet filtering are filtering by address, which is to restrict the flow of packets on source/destination addresses, and filtering by services, which is the flow of packets based on what protocols are involved.

Filtering by address is to allow certain external hosts to talk to certain internal hosts and to prevent an attacker from injecting forged packets into the local network. Its risks are: source address forgery attack, an external host claiming to be a different (trusted) external host, and man in the "middle" forgery attack, to carry out a complete conversation while claiming to be the trusted host.

Filtering by services is looking to the destination port and control which daemons can be accessed. "Each of the tcp services, smtp, nntp, ftp, finger, telnet, login, shell begins by connecting to a socket. The same holds for udp destined for sun rpc, rip and domains daemons. Restricting the destination ports is used. Examples are to deny external udp access to sun rpc (e.g., nfs) and routed but allow domain name service by limiting udp access to port 53 and to allow external access for mail and netnews by limiting tcp access to ports 25 and 119." [6] Risk of the filtering by services is that we can trust the source port only as much as we trust the source machine.

Advantages of packet filtering are [6]:

- One screening router is enough to protect an entire network
- It's doesn't need a user knowledge or cooperation (transparency)
- Widely available in many routers

Disadvantages of packet filtering are [6]:

- Filtering tools are not perfect. They are:
  - Hard to configure
  - Hard to test

♦ Incomplete

- Some protocols are not well suited to packet filtering
- Some security policies can not be enforced by normal packet filtering

Proxying is providing Internet access to a single host while appearing to provide access to all of the internal network's hosts. On the server side for most services, proxying requires appropriate proxy server software. On the client side, it needs custom client software (How to contact the proxy server and how to tell him what real server to connect) or custom user procedures (standard client server to talk to the proxy server).

Advantages of proxying are [6]:

- Users think they're interacting directly with internet services
- Proxy services allow logging to be performed in an effective way.

Disadvantages of proxying are [6]:

- There is a distinct lag between the introduction of a service and the availability of proxying server for it
- Different servers for each service
- It usually requires modifications to clients and/or procedures
- It doesn't work for some services
- It doesn't give a protection from all protocol weaknesses

A firewall is not a complete security solution. It can perform various functions for computer systems' security: focusing, logging, and limiting exposure. But it cannot protect the internal network against malicious insiders, connections that circumvent it (modems), new threats and data-driven attacks (malicious executable code, viruses).

Also there are some techniques to improve the security of the firewalls. These are Tunneling and Virtual Private Network (VPN). Tunneling means to encapsulate network packets (private ones) in another network packets (Internet ones). Software using the same protocol at the two extremities of the tunnel is used in tunneling. Packets are forwarded through Internet. They are compressed and encrypted. VPN technology creates an encrypted communication channel between properly configured machines by using, for example, SSH and PPP. SSH to create a tunnel connection, and then use PPP to run TCP/IP traffic through it. Tunneling can be used between two firewalls or between a firewall and stand-alone remote computer.

A VPN isn't the answer to all security. There are still risks that the computer or network at either end of a VPN could be compromised. A single VPN may not solve all of the problems. If everyone shared the same VPN then the benefits of the Private part would be lost.

Firewalls are not sufficient to ensure security but they are necessary blocks to build a reasonable security wall. Choosing the most appropriate block is also very important. There are two kinds of firewalls [6]: Packet filters or Stateful Multi-Layer Inspection (SMLI) and Application Level Gateways (ALG). The security policy to be implemented determines which type of firewall is the best for a particular Local Area network. Some SMLI firewall examples are Checkpoint system's Firewall-1, Guardian for NT, Cisco system's PIX, Elron firewall. Some ALG firewall examples are TIS's Gauntlet, T-Rex, Altavista firewall, Cisco's Centri firewall, EagleNT and IBM for NT.

But there is no answer to the question, which type of firewall is better. It depends upon the Security Policy specified. Controlling which machines can reach the internal network from outside (SMLI firewalls) and more control over outgoing connections (ALG firewalls). But a tradeoff in choosing ALG firewalls is that they are slower, less flexible but they have greater control.

Firewall can protect against unauthenticated interactive logins from external environment. They block traffic from the outside to the inside and they can protect against any type of network-borne attack. But firewalls can't protect against attacks that don't go through the firewall, and traitors or idiots inside the network it protects.

3.1.1 Firewall Examples

Some examples of firewalls and their qualifications will be explained next. These firewalls are Checkpoint Firewall-1, Gauntlet, T-Rex.

3.1.1.1 Checkpoint Firewall -1

To fully leverage the power and reach of the Internet, organizations must guarantee the protection of all network resources and data. This requires a complete enterprise security solution that protects all elements of an organization—networks, systems, applications and users. Check Point's Secure Virtual Network (SVN) architecture uniquely delivers end-to-end network security enabling organizations to protect business-critical Internet, intranet and extranet traffic.

FireWall-1 is a key component of the SVN architecture and enables network security to be managed with a single enterprise-wide policy. As the industry's most proven security solution, FireWall-1 delivers more than simple access control rules managing traffic into a protected network. Check Point FireWall-1 is a comprehensive security platform that integrates and manages all elements of enterprise security, including [7]:

- Access Control
- User Authentication
- Network Address Translation (NAT)
- Virtual Private Networking (VPN)
- High Availability
- Content Security (anti-virus, URL and Java/ActiveX screening)
- Auditing and Reporting
- LDAP-based User Management
- Intrusion Detection
- Malicious Activity Detection
- Third-party Device Management

Enterprise security can be extended with Check Point's Open Platfonn for Security (OPSEC), providing central integration and management of complementary third-party security applications, services and platforms.

Broad Application Support with Built-in Extensibility Check Point FireWall-1 supports more than 150 pre-defined applications, services and protocols out of the box. Support is provided for all popular Internet services, including the most commonly used applications (HTTP, SMTP, Telnet, FTP, etc.), the entire TCP family of applications and connectionless protocols, such as UDP. In addition, FireWall-1 supports important business applications such as Oracle SQL, multimedia applications such as RealAudio and H.323-based services, like Voice over IP (VoIP).

With its open architecture and powerful INSPECT scripting language, FireWall-1 is extensible to new and custom applications as well. This makes FireWall-1 readily adaptable to special customer needs and evolving security requirements to meet the most rigorous enterprise security demands.

Check Point FireWall-1 is based upon "Stateful Inspection", the de facto standard for Internet firewalls invented by Check Point Software Technologies (U.S. Patent No. 5,606,668 and 5,835,716). "Stateful Inspection" provides the highest level of security possible by incorporating communication- and application-derived state and context information, which is stored and updated dynamically. This provides cumulative data against which subsequent communication attempts can be evaluated. "Stateful Inspection" provides full application-layer awareness without requiring a separate proxy for every service. This results in improved performance, scalability and the ability to support new and custom applications quickly. These are just some of the reasons why customers have adopted "Stateful Inspection" as the firewall technology of choice [7].

"FireWall-1's Network Address Translation feature conceals internal network addresses from the Internet, avoiding their disclosure as public information. In addition to enhancing enterprise security, Network Address Translation enables organizations to maintain unregistered IP addressing schemes and provide Internet access to all users utilizing a single corporate IP address. FireWall-1's advanced address translation capability supports all Internet services." [7]

Today's enterprise networks include not only local corporate users, but also remote locations, mobile workers and telecommuters. Before granting access to sensitive network resources, organizations need a way of validating user authenticity.

"Check Point FireWall-1 meets this requirement with integrated support for three powerful authentication methods and multiple authentication schemes, more than any other security vendor. Users can be authenticated without any modification to server or client applications. And unlike many network security products, FireWall-1 can authenticate users of any IP-based application. FireWall-1's open architecture allows numerous authentication solutions to be integrated into an enterprise-wide security policy, including FireWall-1 passwords, smart cards, token-based products like SecurID, LDAP-stored passwords, RADIUS or TACACS+ authentication servers, X.509 digital certificates and even biometric techniques. In addition, Check Point provides an open application programming interface (API) as part of OPSEC that enables third-party security vendors to develop compatible authentication products." [7]

Check Point FireWall-1 protects users from virus attacks, malicious Java and ActiveX applets and undesirable Web content through its integrated content security capabilities [7]:

- **Integrated Security Servers** – For each connection established through a FireWall-1 HTTP, SMTP or FTP security server, the network manager controls access to specific resources with a high degree of granularity. For example, access can be controlled to specific Web pages and actions, FTP files and operations (e.g., PUT/GET commands), SMTP-specific header fields and more.
- **Third Party Application Support** - Through its support for the OPSEC framework, Check Point FireWall-1 can leverage several open APIs to interface with third-party content security applications. This enables security managers to extend the security of their FireWall-1 installation to provide advanced functionality, such as [7]: "Anti-virus screening to protect internal network resources from viruses that may be contained within incoming traffic. Virus scanning is enabled using the Content Vectoring

Protocol (CVP). URL filtering to block outbound Web requests for inappropriate or unproductive Web content using the URL Filtering Protocol (UFP). Java Security to intelligently screen for malicious executable content leveraging CVP."

- **Malicious Activity Detection** - FireWall-1 can detect malicious activity at the Internet gateway and alert the security manager of attempted violations of the network security policy. FireWall-1's Malicious Activity Detection functionality analyzes FireWall-1 log records to detect a handful of well-known network attacks and indications of suspicious activity.

FireWall-1 provides the underlying platform for Check Point's industry-leading Virtual Private Networking solution—VPN-1 Gateway. Any FireWall-1 installation can be easily upgraded to VPN-1. VPN-1 Gateway can also be purchased as a fully integrated solution incorporating FireWall-1.

Providing full integration of VPN and firewall security, Check Point's VPN-1 delivers a secure and flexible architecture for a complete enterprise-wide VPN deployment [7]:

- **Remote Access VPN** – Mobile and remote users can access corporate network resources via the Internet using VPN-1 SecureClient and VPN-1 SecuRemote client software.
- **Site-to-Site VPN** – VPN-1 Gateway can protect business communications traveling between corporate locations over the Internet or any untrusted IP network.
- **Extranet VPN** – Business partners can safely connect to the company network to run e-Business applications.
- **Client/Server VPN** – Local desktops can establish VPN tunnels with any application server to protect against internal network threats.

Integration of network security and VPN capability eliminates the need to open multiple ports, or "holes," in the firewall to blindly pass VPN traffic as is necessary with many standalone VPN devices. Instead, all controls defined in the FireWall-1 security policy are applied to VPN traffic—guaranteeing complete integrity of network security.

VPN capability is defined as an integral component of an overall enterprise security policy for efficient management and easy deployment.

Check Point's graphical user interface provides a single management console for defining and managing multiple elements of a Secure Virtual Network: firewall security, VPNs, network address translation, bandwidth management and data compression. All object definitions (users, hosts, networks, services, etc.) are shared among all applications for efficient policy creation and security management.

FireWall-1 is designed to deliver scalable security management for all size organizations, from small offices to globally dispersed enterprise networks [7]. With a unique three-tier architecture, a single enterprise-wide security policy can be managed centrally and automatically deployed to an unlimited number of FireWall-1 enforcement points. Automatic policy distribution eliminates the possibility of misconfiguration when managing multiple firewalls.

"Check Point FireWall-1 can be easily deployed throughout an organization for true enterprise security. For organizations (enterprise networks or managed service providers) requiring separate security policies for independent business units or customers, Check Point offers Provider-1. With Provider-1, multiple FireWall-1 security policies can be managed from a single console, while maintaining complete isolation of security and user databases." [7]

- **Unparalleled Platform Support** - Check Point's patented Stateful Inspection technology enables FireWall-1 to be deployed on a variety of operating systems and platforms for maximum flexibility and security [7]:
  - ♦ Server Operating Systems
    - Hewlett-Packard HP-UX
    - IBM AIX
    - Linux
    - Microsoft Windows NT
    - Microsoft Windows 2000
    - Sun Microsystems Solaris
  - ♦ Check Point VPN-1 Appliances
  - ♦ Third-party security appliances, routers and switches

The Open Platform for Security (OPSEC) extends Check Point's Secure Virtual Network architecture by providing a unique, open platform for integration and interoperability. Over 200 companies have adopted its enterprise integration interfaces to develop complete integrated Internet security solutions. The choice of best-of-breed products and services offers customers the flexibility to design an e-Business security architecture that matches the challenges unique to the company's own network and business needs. [7]

- **Integrated Internet Security** – "Check Point protects the customer investment in VPN-1/FireWall-1 by continually updating and defining new integration interfaces for key technologies including PKI, directories, authentication, content security, intrusion detection and others. Using the OPSEC Software Development Kit (SDK) and industry protocols, vendors and customers connect easily to the SVN architecture. Rigorous testing for OPSEC certification guarantees seamless integration with VPN-1/FireWall-1, eliminating the questionable interoperability of single suite products. OPSEC also delivers the value of plug-and-play security technology to enable a true multi-layered enforcement structure, incorporating a wide range of technologies to protect data, applications and users. OPSEC is leading the industry to provide the integrated Internet security needed to take full advantage of the promise of e-Business." [7]
- **Broad Choice of Network Configurations** – "A growing number of Internet Service Providers have implemented OPSEC-compliant products with VPN-1/FireWall-1 to deliver a wide range of managed security services to customers seeking to outsource their security and VPN services. For the corporate network, Check Point offers the most versatile choices for best-of-breed infrastructure deployment platforms in the security industry. Organizations can deploy Check Point's security solutions on routers, appliances, systems, switches and other internetworking devices. This flexibility allows customers to leverage their existing hardware investment, enabling secure e-Business." [7]

Check Point FireWall-1 is much more than just a firewall. It is a complete platform for integrating all aspects of enterprise security. FireWall-1 interoperates with multiple applications and supports a variety of functional modules to provide the industry's only solution for Secure Virtual Networking.

The management features of Checkpoint Firewall-1 are [7]:

- **Reporting:** The Check Point Reporting Module generates custom and pre-defined reports from FireWall-1 log data for comprehensive security auditing, activity trending and accounting.
- **LDAP:** The Account Management Module enables FireWall-1 to query LDAP-compliant directory servers for user-level security information that is used to enforce elements of the enterprise security policy, such as user authentication, data encryption and access control privileges.
- **Router Security Management:** The Open Security Extension™ enables security policies for routers and other third-party security devices to be defined, deployed and managed centrally eliminating point-to-point configuration and manual definition of access control lists (ACLs).

The VPN and security modules of Firewall-1 are [7]:

- **VPN:** Check Point's VPN-1 product family is based on FireWall-1 and provides a complete solution set for enterprise VPN deployments. Solutions include software-based VPN gateway products, VPN appliances, client-based VPN software, VPN acceleration cards and turnkey Public Key Infrastructure (PKI) products.
- **Intrusion Detection:** Check Point RealSecure is a real-time attack recognition and response system, providing proactive network protection from attacks or misuse. It recognizes more than 300 types of attacks and responds by automatically reconfiguring FireWall-1 to terminate connections and protect against future attacks.

The performance and reliability of Firewall-1 can be described as [7]:

- **Quality of Service:** FloodGate-1 is a policy-based bandwidth management solution that can integrate with FireWall-1 to ensure reliable performance for business-critical traffic on VPN, private WAN and Internet links.
- **High Availability:** Check Point's High Availability Module delivers seamless connectivity in the event of a gateway failure. Advanced firewall synchronization is leveraged to maintain connections during FireWall-1 gateway fail-over.
- **Server Load Balancing:** Connect Control enables FireWall-1 to deliver application server load balancing by distributing incoming connections across a pool of

application servers for improved user response times and enhanced network connectivity.

- **Compression:** The Check Point Compression Module significantly increases the performance and capacity of network infrastructures by compressing data at policy enforcement points

"Firewall-1 can operate on operating systems; Microsoft Windows NT 4.0 (SP4, SP5 and SP6), Sun Solaris 2.6, Solaris 7 (32 bit only), Red Hat Linux 6.0, 6.1,HP-UX 10.20, 11.0 (32 bit only),and IBM AIX 4.2.1, 4.3.2. Firewall-1 also supports the hardware platforms of Check Point VPN-1 Appliances, ODS SecurCom 8000 family, Alcatel (Xylan) switches, Nortel ARN, ASN, BN and System 5000 routers, and Nortel Contivity switches. Firewall-1 requires 40 MegaBytes of disk space and a memory of 64 MB min.for Management Server and 128 MBs for Enforcement Module *128 MB*. Also 32 MBs is needed for GUI Client. Firewall-1 requires a network interface of type ATM, Ethernet, Fast Ethernet, FDDI or Token Ring." [7]

3.1.1.2 Gauntlet Firewall 6.0

"Gauntlet Firewall carefully watches everything that attempts to pass by and letting you selectively decide what gets in and what gets out. Gauntlet Firewall can guard one door or many doors, making it ideal for protecting small, medium, or large size networks with one site or multiple sites around the world. " [8]

For securely transferring data between multiple sites and remote users the included Gauntlet VPN can be used to ensure privacy of communications. VPN is not an add-on in Gauntlet Firewall, it is included at no additional cost. Gauntlet VPN uses the Internet to send encrypted data from the gatekeeper at the main door to traveling employees, off-site engineers, and other corporate sites with no compromise in security and immediate return of investment.

The Single rule view feature uses "one screen to review, add and edit security rules for groups and objects - eliminating the need to search multiple screens for firewall and policy information." [8] This eliminates the need to edit firewall rules individually and enables to add and edit rules on multiple firewalls easily. Variable administration privilege provides multiple levels of administrative control from multiple locations, allowing local offices to edit rules based on permissions set.

The New Global Enterprise Management System (GEMS) add-on complements Gauntlet v6.0 by enabling worldwide deployment, administration, and management of as many as 500 Gauntlet firewalls and VPN devices.

With the inclusion of Crystal Reports and the new logging daemon, Gauntlet reporting has greatly improved and now utilizes four different log files, Applications, VPN, Kernel and Statistics. The Rule View allows to control the logging level for each rule, enabling to decide what to log. With the GEMS add-on, the ability to see a consolidated view of all firewall logs is added..

In Gauntlet 6.0, "Gauntlet Virtual Private Networking (VPN) integrated with Gauntlet firewall. Single rule view allows reviewing firewall and policy rules from a single screen. The Graphical User Interface (GUI) is enhanced. Variable administration privilege with multiple levels of administrative control from multiple locations is added. UDP Proxy support is included and also RTSP-PDK Proxy support is added. Logging and reporting systems are enhanced and Multi Bind Address and port pairs are used. There is a new authentication mechanism. And Single Sign On Global Enterprise Management System(GEMS) is now an add-on." [8]

The Gauntlet v6.0 Features & Benefits are [8]:

- **Gauntlet Firewall offers flexible protection** - Gauntlets' unique architecture allows the administrator to flexibly mix and match packet filtering, application proxy, or adaptive proxy technology within a single application.

- **New Single Rule View eases administration** - Single rule view uses one screen to review security rules - eliminating the need to search multiple screens for firewall and policy information. The Graphical User Interface (GUI) provides a quick, effective method of adding, deleting, or modifying firewall rules for a user or group.

- **Variable Administration provides distributed firewall control** - Managing hundreds of firewall and Virtual Private Networking (VPN) devices is a difficult task. The new Variable administration feature provides permission based firewall control for easier and more consistent distributed policy management.

- **UDP Proxy adds connectionless protocol support** - This new proxy handles most UDP-based protocols. Pre-defined configurations for DNS, NTP, NetBIOS, Syslog, TFPT, and WINS are supplied. The proxy creates its own concept of a UDP connection, which supplies better security and enables logging of traffic that was previously unloggable.

- **RTSP-PDK Proxy support** - This new proxy handles traffic that uses the RTSP protocol such as Real Audio's G2 and Apple's Quicktime. The proxy includes both TCP and UDP support and supports the Adaptive Proxy functionality for improved performance. It is also possible to enable bandwidth throttling for individual configuration sets to limit connection usage from specific sources.

- **Global Enterprise Management System (GEMS) add-on reduces network complexity** - The Global Enterprise Management System (GEMS) is an affordable, scalable management tool that seamlessly integrates with Gauntlet v6.0. GEMS can be installed on Windows 98, Windows NT, and Windows 2000 machines and enables worldwide deployment, administration, and management of up to 500 firewalls and/or Virtual Private Networking devices.

- **Re-designed logging feature enhances reporting** - Enhanced logging feature enables granular control over firewall reporting. Gauntlet v6.0 adds distinctive packet filter logging and bundling of Crystal Reports for more extensive reporting. Also, the addition of the new logging daemon provides more functionality than the traditional syslog daemon. The new daemon utilities four different log files - one each for Applications, VPN, Kernel, and Statistics. The Rule View in the GUI allows you to control the logging level for each rule.

- **Gauntlet Virtual Private Networking (VPN) is now tightly integrated** - Gauntlet Virtual Private Networking (VPN) is no longer installed as an add-on module - simplifying VPN administration.

- **IPSec VPN compliance ensures compatibility with other popular IPSec VPN's** - Gauntlet is ICSA IPSec compliant, assuring successful VPN deployments with other popular IPSec VPN manufacturers. Gauntlet's VPN technology provides an easy, affordable, and secure means for businesses to securely communicate with each other.

- **Mode-config/Virtual Identity facilitates remote end-user access** - Mode-config gives remote VPN users transparent access to their local networking resources. Gauntlet's virtual identity allows remote VPN clients to authenticate once, which decreases your wait time and saves valuable bandwidth.

- **Single Sign-On simplifies authentication** - Single Sign-On allows a user to authenticate only once through the firewall for access to other services on the network. Single Sign-On reduces the number of times a user would have to authenticate to other corporate applications within the network. This streamlines the authentication process for internal users. With Single Sign-On, internal users will no longer have to authenticate separately for each proxy.

- **McAfee guards your network from virus mutations** - Gauntlet integrates the McAfee Anti-Virus software for protection against viruses. Corporations will receive automatic updates as new cures are released to protect against the latest virus outbreaks.

- **McAfee scanning improvements increase Anti-Virus/SMTP performance** - Gauntlet was tuned to enhance the SMTP performance. As a result of these and other improvements, Gauntlet improves Anti-Virus scanning performance by 40%.

- **Gauntlet internal re-design improves Web/HTTP performance** - Adjusting the Firewall gateway process of the Gauntlet v6.0 has lead to an HTTP performance increase of 10%.

- **Professional service provides additional security expertise** - PGP Security's experienced staff of security experts can help organization of any size with their security needs. Talking directly to our support engineer shortens response time and reduces the complexity of supporting multiple products from different manufacturers. Small, medium, or large corporations can call one number for all their support issues.

The system requirements of Gauntlet firewall are [8]:

- **For Sun:** Solaris 8 operating system UltraSPARC or Enteprise Class system - 128 MB of RAM (more is strongly recommended), 4GB of free disk space
- **For Hewlett Packard:** HP-UX 11 operating system 64-bit HP PA-RISC system - 128 MB of RAM (more is strongly recommended), 4GB of free disk space

3.1.1.3 T-Rex Security Suit

The T-Rex Firewall is a highly integrated enterprise security suite that combines functions that normally require the installation of multiple products. Its functions are [9]:

- Access control
- Authentication
- Extensible Application controls via application specific APIs.
- Hardware assisted Virtual Private Network (VPN)
- Network Address Translation (NAT)
- Content Filtering (URL, Java, ActiveX, JavaScripts, SPAM)
- Fault tolerant High Availability Option (99.999% availability)
- Workload Balancing
- Non-disruptive hardware and software modifications
- Extensive auditing and reporting tools that can produce more than 52 unique reports
- Real-time performance monitor
- Network scanning and intrusion detection tools
- Totally automated operations to minimize administration overhead.

The T-Rex functions can be described as [9]: "T-Rex provides unequaled scalability to meet the requirements of small, large and ultra-large organizations. Its performance supports more than a gigabit/second throughput. Hardware assisted IPSec VPN provides encrypted communications without sacrificing system throughput. It provides support for hundreds of services and applications. T-Rex provides organizations with the ability to define a single security policy that can be distributed across multiple firewalls from a single administration workstation. T-Rex is an advanced hybrid firewall designed to repel the most sophisticated attacks from skilled and determined crackers. Application specific proxies block application based attacks that pass unnoticed through the best of the stateful packet filters. The proxy API's also allow local customization to fine tune security controls for third party applications.

The T-Rex fault-tolerant architecture provides multiple levels of error detection, reporting and recovery. The "fail-safe" architecture blocks the flow of traffic when an error occurs thus preventing accidental violations of the security policy. Unlike packet filter firewalls that can fail-open in the event of a hardware or software error T-Rex will fail shut blocking unauthorized traffic. T-Rex logs and controls all traffic between secured and unsecured networks. T-Rex can be configured to match the security policies of an organization instead of imposing its own policy upon an organization. T-Rex is easy to install, configure, maintain and use. T-Rex works with shrink wrapped applications to provide easy and transparent access from secured to unsecured (Internet) networks."

"T-Rex is available on AIX, HP-UX, Linux, and Solaris (SPARC and Intel) systems. In addition it is available on a variety of embedded systems using PowerPC, UltraSPARC and Intel architectures." [9] T-Rex runs on single and multi-processor systems as well as clusters of SMP systems. T-Rex's key benefits are [9]:

- Prevent unauthorized access to protected networks
- Prevent unauthorized modification or destruction of secured data
- Defend against Denial of Service Attacks
- Log and report network usage including break-in attempts
- Prevent unscheduled outages that deny access to servers
- Balance workloads across multiple servers improving performance

- Improve service availability with dynamic traffic re-direct.
- Mach 3 Performance

The T-Rex firewall is a highly integrated enterprise security suite that combines functions that normally require the installation of multiple products. Its hybrid architecture provides maximum security and performance. Application specific proxies provide high levels of security and access control tailored for the application. The Application Program Interface (API) allows site specific extensions to the application proxy. This provides fine grain application control beyond the standard product. Stateful Packet Filters can also be employed for applications that do not require the same level of security. A circuit level proxy is also provided for additional flexibility. This unprecedented flexibility allows the security administrator to configure the firewall to meet their unique site requirements.

The T-Rex network security suite derived from technology that has been securing large organizations for more than five years. It uses technology developed by dozens of experts from around the world. Making T-Rex an open source project ensures that it will continue to remain state-of-the-art. Use of open source means it will be subjected to wide scale peer review by leading experts. This process will provide users with greater reliability, more security features and faster response to new security threats. It also makes the firewall more affordable.

Install scripts on the CD-ROMs automatically harden the operating system while installing the T.Rex software. This allows installations in less than 10 minutes. The multi-tiered support structure offered by FAS allows customers to choose the level of support they require. This makes the product very affordable.

The main technologies found in T-Rex include [9]:

- Application specific proxies for E-mail (SMTP, POP3), File Transfer (FTP), World Wide Web (HHTP, SHHTP, SSL), Terminal Services (Telent, TN3270), X Window System (X11), and Real Audio & Real Video
- Advanced Application proxy with extensible application controls via an API.

- A generalized RPC and UDP proxy
- Hardware assisted Virtual Private Network (VPN)
- Network Address Translation (NAT)
- Socks V4 & V5 Circuit Gateway
- E-mail controls
- Stateful Packet Filtering
- Integrated Content Filtering (URL, Java, ActiveX, JavaScripts, SPAM)
- Integrated fault tolerant High Availability Option (99.999% availability)
- Integrated Workload Balancing
- High Speed Caching
- Split DNS
- Intrusion Monitoring and Detection
- Graphical User Interface
- Network Scanners
- Integrated Authentication Servers
- Built-in monitors for detecting attacks, checking system and network integrity and performance and capacity,
- Automated operations including automatic log management and report generation

T-Rex provides unequaled scalability to meet the requirements of small, large and ultra-large organizations. T-Rex supports more than a gigabit/second throughput. Hardware assisted IPSec VPN provides encrypted communications without sacrificing systems throughput. It provides support for hundreds of services and applications. T-Rex provides organizations with the ability to define a single security policy that can be distributed across multiple firewalls from a single administration workstation.

3.1.2 Firewalls and GASSP Principles

Some of the Generally Accepted System Security Principles (GASSP) can be used in developing and using firewalls in the process of avoiding the attacks to our system. GASSP principles are in hierarchical order, which is from pervasive to detailed. The relevant GASSP principles are Access Control Broad Functional Principle, and Network and Infrastructure Security Broad Functional Principle. These principles of GASSP can be used in implementing and configuring firewalls in order to protect the computer system of an organization. Also a detailed security principle can be formed for vulnerability scanners.

The access to the system from the outer world can be limited to only authorized sites or IPs by using firewalls. By using the Access Control Broad Functional Principle the firewall can be configured to balance the access to information assets and supporting Information Technology resources.

Firewalls can be used to learn the impacts of the Internet to the information system and to reveal the vulnerabilities raised because of the Internet. The attempts of attack to the information system from internet can be prevented by using a good configured firewall. And such a configuration can be implemented by using Network and Infrastructure Broad Functional Principle as a guide.

3.1.2.1 Developed Detailed Security Principle About Firewalls

The principle can be stated as, *"Use firewalls in the process of preventing the attacks coming from outside to the organization's information system."* Firewalls are able to prevent the types of attacks, which are possible for an organization's network by denying the connections to the system in regard to their configurations. As seen above firewalls are used in avoidance layer of the intrusion management systems for preventing the system from the attacks. The GASSP principles about this process' point out the firewalls.

3.2 Vulnerability Scanners

Vulnerability scanners can be used in assurance layer of intrusion management systems, and while using and developing such scanners GASSP principles can be used and GASSP detailed security principle about vulnerability scanners can be developed.

Many end-users, such as employees within a company, should not have access to each other's machines, to administrative functions, to network devices or similar rights. Of course in practice this is usually not achieved, and a user with minimal skills will be able to do a successful penetration and achieve remote administrative rights of your network within a few minutes of exploration.

Because of the amount of flexibility needed for normal operation, internal networks can not afford maximum security. However with no security at all, internal users can be a major threat for many corporate internal networks. A user within the company already has access to many resources and does not need to bypass firewalls or other security mechanisms which prevent non-trusted sources, such as Internet users, to access the internal network. Such internal users can also make sure that it is hard enough to identify or even detect.

Other than internal users, poor network security will mean that once a hacker gets hold of a computer which is within your network, he or she also has access to the rest of the Internal Network. Many holes exist which allow hackers to tunnel through different protocols, such as SMTP (e-mail) and HTTP, to bypass security mechanisms such as firewalls and bastion hosts. Such attacks will allow a more sophisticated attacker to easily penetrate and get administrative rights over an internal network, meaning confidential e-mails and documents can be read, computers can be trashed leading to loss of information, possible business information leakage and other problems. All these vulnerable points require a vulnerability check for the whole system. This check can be done via Vulnerability Scanner tools.

Vulnerability scanning is the process of checking for all the potential methods that an attacker might use to tamper with an organization's network. By analyzing what types of software and software configurations are on a given network, scanners are able to determine what types of attack are possible against a network so it can defend itself accordingly. Vulnerability scanning has become a primary focus of network administrators as the potential threat of a security breach has become preeminent. Network and software vulnerabilities exist in two basic forms: known vulnerabilities and unknown vulnerabilities. Known vulnerabilities are those that have been identified and isolated by a security scan. An advisory is then published to alert users of the existing hole or flaw. Unknown vulnerabilities have not been discovered or publicly acknowledged, making them a potential security threat. Many vulnerability scanners are able to check both known and unknown vulnerabilities.

3.2.1 Vulnerability Scanner Examples

Some examples of vulnerability scanners and their qualifications will be explained next. These vulnerability scanners are eEye Retina, Languard, and Nessus.

3.2.1.1 eEye Retina

Retina is a network vulnerability scanner. While most security scanners confine themselves to searching for only known vulnerabilities, Retina shatters the mold of the typical security scanner through its use of Artificial Intelligence(AI). The AI component allows Retina to think like a hacker or security analyst would if they were attempting to break into your network. Retina searches for both known and unknown vulnerabilities.

Retina discovered a hole in Microsoft Internet Information Sever. Using Retina, a hole that affected over a million Windows NT web servers on the Internet was identified. A serious flaw, which left unchecked, could have been devastating. Retina has been the force behind several other high-profile vulnerability advisories including a flaw in Ultraseek, the Infoseek search engine.

Retina has the ability to scan, monitor and fix vulnerabilities within a network's Internet, Intranet, and Extranet. Thus, giving the network administrator complete control across all possible points of attack within an organization and the confidence required in operating a network to its fullest potential. Retina includes easy-to-navigate reporting tools to help identify and isolate high priority fixes, allowing total command over auditing network security and open network gateways into an internal network.

Retina is designed to identify and alert security vulnerabilities, suggest fixes and report possible security holes within a network's Internet, Intranet and Extranet systems. Its scanning capabilities provide a network security analysis. Retina includes vulnerability auditing modules for the following systems and services [10]:

- NetBIOS
- HTTP, CGI and WinCGI
- FTP
- DNS
- DoS vulnerabilities
- POP, SMTP and LDAP
- TCP/IP and UDP
- Registry
- Services
- Users and Accounts
- Password vulnerabilities
- Publishing extensions
- Database servers
- Firewalls and Routers
- Proxy Servers

"Retina can produce fully documented network audit reports based on its security scans. Smart reporting allows the network administrator to access, read and print these real-time security test results with ease. The reports detail all security holes and flaws that are detected in a scan and are ready to print. Two options are available for reporting: the Technical Report with intricate detail to satisfy IT personnel, and the Executive Report for high-level management summaries." [10]

3.2.1.2 Languard

LANguard is a vulnerability scanner from GFI. Languard can enumerate possible entry points such as , "Rogue services and open ports, SNMP holes, rogue or backdoor users, Trojan Horses or backdoor software, open shares, weak network passwords, and enumeration of users, services etc." [11]

The methods of Languard used in its operation are "Information gathering, operating system identification, known security issues in software packages, live host detection, any hot fixes installed, and registry entries." [11]

In rising alerts, well known security issues are immediately recognized and also intelligent scanning methods are used. The output can be given in the formats of HTML and XML. Also it has the ability to compare scans, to learn about new possible entry points.

Extra Features of Languard can be stated as, "exploitation of NETBIOS vulnerability in Windows 95,98 and ME, SNMP auditing, trace route, DNS lookup, remote machine shutdown and sending spoofed messages (social engineering techniques used in hacking)." [11]

3.2.1.3 Nessus

Nessus is a vulnerability scanner from the NESSUS Corp. It can be freely downloaded. The main features of Nessus Security Scanner are [12]:

- **Plug-in architecture** – "Each security test is written as an external plug-in. This way, you can easily add your own tests without having to read the code of the nessusd engine. The complete list of the Nessus plug-ins is online and can be found on internet."

- **NASL** – "The Nessus Security Scanner includes NASL, (Nessus Attack Scripting Language) a language designed to write security test easily and quickly (security checks can also be written in C)."

- **Up-to-date security vulnerability database** – "Nessus mostly focus on the development of security checks for recent security holes. Security checks database is updated on a *daily* basis and all the newest security checks are available on FTP servers and mirrors."

- **Client-server architecture** – "The Nessus Security Scanner is made up of two parts: A server, which performs the attacks, and a client which is the front-end. We can run the server and the client on different systems. That is, auditing whole network from a personal computer can be done, whereas the server performs its attacks from the main frame which is upstairs. There are several clients: one for X11, one for Win32 and one written in Java."

- **Ability to test an unlimited amount of hosts at the same time** – "Depending on the power of the station running the Nessus server, test of two, ten or forty hosts can be done at the same time."

- **Smart service recognition** – "Nessus does not believe that the target hosts will respect the Internet Assigned Numbers Authority (IANA) assigned port numbers. This means that it will recognize a FTP server running on a non-standard port (for instance 31337), or a web server running on port 8080."

- **Multiples services** – "If two web servers (or more) is running on the same host, one on port 80 and another on port 8080. Nessus will test both of them."

- **Coordinated tests** – "The security tests performed by Nessus cooperate so that nothing useless is made. If FTP server does not offer anonymous logins, then anonymous-related security checks will not be performed."

- **Cracker behavior** – "Nessus does not believe that version x.y.z of a given software is immune to a specific or any security problem. 95% of the security checks will actually perform their job - they'll try to overflow your buffers, relay some mails, and even to crash down the computer!"

- **Reports with guidance** – "Nessus will not only tell you what's wrong on your network, but will, most of the time, tell you how to prevent crackers from exploiting the security holes found and will give you the risk level of each problem found (from *Low* to *Very High*)."

- **Exportable reports** – "The Unix client can export Nessus reports as ASCII text, LaTeX, HTML, HTML (with pies and graphs) and an easy-to-parse file format."

- **Multilingual support** – "Nessus can issue reports in English or in French. More languages are to come."

- **Independent developers** – "The Nessus developers are independent from the rest of the world, so we will not hide a security vulnerability in the program XYZ because we have a contract with them."

- **Easy-to-reach developers** – "The contact with the developers can be implemented easily."

3.2.2 Vulnerability Scanners and GASSP Principles

Some of the Generally Accepted System Security Principles (GASSP) can be used in developing and using vulnerability scanners in network security analysis, and system security checks. Also vulnerability scanners should be used in information security policy development. GASSP principles are in hierarchical order, which is from pervasive to detailed. The relevant GASSP principles are Assessment Pervasive Principle, Information Risk Management Broad Functional Principle, Network and Infrastructure Security Broad Functional Principle, and Operational Continuity and Contingency Planning Broad Functional Principle. These principles of GASSP can be used in vulnerability checking processes of the information systems' of an organization. These principles are generally about checking the vulnerabilities and risks on the Information System. Also a detailed security principle can be formed for vulnerability scanners.

The risks to information and information systems should be assessed periodically, because the information and risks to the information changes everytime. So there should be a periodic assessment of the vulnerable points in the system. Checking the vulnerable points of the system can assess risks and vulnerability scanners can be used for this assessment in the guidance of the Assessment Pervasive Principle.

Vulnerability scanning tools also give possible measures for the vulnerable points of the system they checked, and they can help taking measures. To choose effective and efficient information security measures, management must identify the assets to be protected, the threats to the assets, and the vulnerability of the assets or their environment to the threats. While developing and choosing a vulnerability scanner, Information Risk Management Broad Functional Principle should also be taken into account.

Vulnerability scanners can be used to learn the impacts of the internet to the information system and to reveal the vulnerabilities risen because of the internet. In this process the guidance of Network and Infrastructure Security Broad Functional Principle plays an important role too.

To preserve the continuity of the information system all the risks and vulnerable points of the system should be known and necessary measures should be taken. In this process vulnerability scanners must be used. And Operational Continuity and Contingency Planning Broad Functional Principle takes an important role in this process too.

3.2.2.1 Developed Detailed Security Principle About Vulnerability Scanners

The principle can be stated as, *"Use vulnerability scanner programs in the process of checking all of the potential methods that an attacker might use to tamper with an organization's network."* Vulnerability scanners are able to detennine the types of attacks, which are possible for an organization's network, by analyzing network's software types and software configurations. Both known and unknown vulnerabilities can be checked by many of the vulnerability scanners. As seen above vulnerability scanners are used in vulnerability assessment process of the information systems and they play an important role in this process. The GASSP principles about this process' point out the vulnerability scanner tools and vulnerability scanning.

3.2.3 Intrusion Detection Systems

Intrusion detection can be describe as, "Pertaining to techniques which attempt to detect intrusion into a computer or network by observation of actions, security logs, or audit data. Detection of break-ins or attempts either manually or via software expert systems that operate on logs or other information available on the network." [1] Intrusion

Detection Systems (IDS) resides in the detection layer of the intrusion management systems and plays an important and key role in this layer.

Intrusion detection systems help computer systems prepare for and deal with attacks. They accomplish this goal by collecting information from a variety of system and network sources, then analyzing the information for symptoms of security problems. In some cases, intrusion detection systems allow the user to specify real-time responses to the violations. Intrusion detection systems perform a variety of functions [13]:

- Monitoring and analysis of user and system activity
- Auditing of system configurations and vulnerabilities
- Assessing the integrity of critical system and data files
- Recognition of activity patterns reflecting known attacks
- Statistical analysis for abnormal activity patterns
- Operating system audit trail management, with recognition of user activity reflecting policy violations

Some systems provide additional features, including [13]:

- Automatic installation of vendor-provided software patches
- Installation and operation of decoy servers to record information about intruders.

The combination of these features allows system managers to more easily handle the monitoring, audit, and assessment of their systems and networks. This ongoing assessment and audit activity is a necessary part of sound security management practice.

Intrusion Detection Systems are security management tools that [13]:

- Collect information from a variety of system sources,
- Analyze that information for patterns reflecting misuse or unusual activity,
- In some cases, automatically respond to detected activity, and
- Report the outcome of the detection process.

3.2.3.1 Major Types of Intrusion Detection Systems

Many IDSs can be described in terms of three fundamental functional components [14]:

- **Information Collection** -- the different sources of event information used to determine whether an intrusion has taken place. These sources can be drawn from different levels of the system, with network, host, and application monitoring most common.
- **Analysis** – the part of intrusion detection systems that actually organizes and makes sense of the events derived from the information sources, deciding when those events indicate that intrusions are occurring or have already taken place. The most common analysis approaches are *misuse detection* and *anomaly detection.*
- **Response** – the set of actions that the system takes once it detects intrusions. These are typically grouped into active and passive measures, with active measures involving some automated intervention on the part of the system, and passive measures involving reporting IDS findings to humans, who are then expected to take action based on those reports.

There are several design approaches used in Intrusion Detection. These drive the features provided by a specific IDS and determine the detection capabilities for that system. For those who must evaluate different IDS candidates for a given system environment, these approaches can help them determine what goals are best addressed by each IDS [14].

3.2.3.1.1 Information Collection

The most common way to classify IDSs is to group them by information source. Some IDSs analyze network packets, captured from network backbones or LAN segments, to find attackers. Other IDSs analyze information sources generated by the operating system or application software for signs of intrusion.

- **Network-Based Intrusion Detection Systems** - The majority of commercial intrusion detection systems are network-based. These IDSs detect attacks by capturing and analyzing network packets. Listening on a network segment or switch, one network-based IDS can monitor the network traffic affecting multiple hosts that are connected to the network segment, thereby protecting those hosts. Network-based IDSs often consist of a set of single-purpose sensors or hosts placed at various points in a network. These units monitor network traffic, performing local analysis of that traffic and reporting attacks to a central management console. As the sensors are limited to running the IDS, they can be more easily secured against attack. Many of these sensors are designed to run in "stealth" mode, in order to make it more difficult for an attacker to determine their presence and location.

Advantages of Network-Based IDSs are [14]:

- A few well-placed network-based IDSs can monitor a large network.
- The deployment of network-based IDSs has little impact upon an existing network. Network-based IDSs are usually passive devices that listen on a network wire without interfering with the normal operation of a network. Thus, it is usually easy to retrofit a network to include network-based IDSs with minimal effort.
- Network-based IDSs can be made very secure against attack and even made invisible to many attackers.

Disadvantages of Network-Based IDSs are [14]:

- Network-based IDSs may have difficulty processing all packets in a large or busy network and, therefore, may fail to recognize an attack launched during periods of high traffic. Some vendors are attempting to solve this problem by implementing IDSs completely in hardware, which is much faster. The need to analyze packets quickly also forces vendors to both detect fewer attacks and also detect attacks with as little computing resource as possible, which can reduce detection effectiveness.
- Many of the advantages of network-based IDSs don't apply to more modern switch-based networks. Switches subdivide networks into many small segments (usually one fast Ethernet wire per host) and provide dedicated links between hosts serviced by the same switch. Most switches do not provide universal monitoring ports and this limits the monitoring range of a network-based IDS

sensor to a single host. Even when switches provide such monitoring ports, often the single port cannot mirror all traffic traversing the switch.

- Network-based IDSs cannot analyze encrypted information. This problem is increasing as more organizations (and attackers) use virtual private networks.
- Most network-based IDSs cannot tell whether or not an attack was successful; they can only discern that an attack was initiated. This means that after a network-based IDS detects an attack, administrators must manually investigate each attacked host to determine whether it was indeed penetrated.
- Some network-based IDSs have problems dealing with network-based attacks that involve fragmenting packets. These malformed packets cause the IDSs to become unstable and crash.

• **Host-Based Intrusion Detection Systems** - Host-based IDSs operate on information collected from within an individual computer system. "This vantage point allows host-based IDSs to analyze activities with great reliability and precision, determining exactly which processes and users are involved in a particular attack on the operating system." [14] Furthermore, unlike network-based IDSs, host-based IDSs can see the outcome of an attempted attack, as they can directly access and monitor the data files and system processes usually targeted by attacks. Host-based IDSs normally utilize information sources of two types, operating system audit trails, and system logs. Operating system audit trails are usually generated at the innermost (kernel) level of the operating system, and are therefore more detailed and better protected than system logs. However, system logs are much less obtuse and much smaller than audit trails, and are furthermore far easier to comprehend. Some host-based IDSs are designed to support a centralized IDS management and reporting infrastructure that can allow a single management console to track many hosts. Others generate messages in formats that are compatible with network management systems.

Advantages of Host-Based IDSs are [14]:

- Host-based IDSs, with their ability to monitor events local to a host, can detect attacks that cannot be seen by network-based IDS.
- Host-based IDSs can often operate in an environment in which network traffic is encrypted, when the host-based information sources are generated before data is

encrypted and/or after the data is decrypted at the destination host. Host-based IDSs are unaffected by switched networks.

- When Host-based IDSs operate on OS audit trails, they can help detect Trojan Horse or other attacks that involve software integrity breaches. These appear as inconsistencies in process execution.

Disadvantages Host-Based IDSs are [14]:

- Host-based IDSs are harder to manage, as information must be configured and managed for every host monitored.
- Since at least the information sources (and sometimes part of the analysis engines) for host-based IDSs reside on the host targeted by attacks, the IDS may be attacked and disabled as part of the attack.
- Host-based IDSs are not well suited for detecting network scans or other such surveillance that targets an entire network, because the IDS only sees those network packets received by its host.
- Host-based IDSs can be disabled by certain denial-of-service attacks.
- When host-based IDSs use operating system audit trails as an information source, the amount of information can be immense, requiring additional loca' storage on the system.
- Host-based IDSs use the computing resources of the hosts they are monitoring, therefore inflicting a performance cost on the monitored systems.

- **Application-Based Intrusion Detection Systems** - Application-based IDSs are a special subset of host-based IDSs that analyze the events transpiring within a software application. The most common information sources used by application-based IDSs are the application's transaction log files. The ability to interface with the application directly, with significant domain or application-specific knowledge included in the analysis engine, allows application-based IDSs to detect suspicious behavior due to authorized users exceeding their authorization. This is because such problems are more likely to appear in the interaction between the user, the data, and the application.

Advantages Application-Based IDSs are [14]:

- Application-based IDSs can monitor the interaction between user and application, which often allows them to trace unauthorized activity to individual users.
- Application-based IDSs can often work in encrypted environments, since they interface with the application at transaction endpoints, where information is presented to users in unencrypted form.

Disadvantages Application-Based IDSs are [14]:

- Application-based IDSs may be more vulnerable than host-based IDSs to attacks as the applications logs are not as well protected as the operating system audit trails used for host-based IDSs.
- As Application-based IDSs often monitor events at the user level of abstraction, they usually cannot detect Trojan Horse or other such software tampering attacks. Therefore, it is advisable to use Application-based IDS in combination with Host-based and/or Network-based IDSs.

3.2.3.1.2 Intrusion Detection System Analysis

"There are two primary approaches to analyzing events to detect attacks: misuse detection and anomaly detection. Misuse detection, in which the analysis targets something known to be "bad", is the technique used by most commercial systems. Anomaly detection, in which the analysis looks for abnormal patterns of activity, has been, and continues to be, the subject of a great deal of research. Anomaly detection is used in limited form by a number of IDSs. There are strengths and weaknesses associated with each approach, and it appears that the most effective IDSs use mostly misuse detection methods with a smattering of anomaly detection components." [14]

- **Misuse Detection -** Misuse detectors analyze system activity, looking for events or sets of events that match a predefined pattern of events that describe a known attack. As the patterns corresponding to known attacks are called *signatures*, misuse detection is sometimes called "signature-based detection." The most common form of misuse detection used in commercial products specifies each pattern of events corresponding to an attack as a separate signature. However, there are more sophisticated approaches to doing misuse detection (called "state-based" analysis techniques) that can leverage a single signature to detect groups of attacks.

Advantages of Misuse Detection are [14]:

- Misuse detectors are very effective at detecting attacks without generating an overwhelming number of false alarms.
- Misuse detectors can quickly and reliably diagnose the use of a specific attack tool or technique. This can help security managers prioritize corrective measures.
- Misuse detectors can allow system managers, regardless of their level of security expertise, to track security problems on their systems, initiating incident handling procedures.

Disadvantages of Misuse Detection are [14]:

- Misuse detectors can only detect those attacks they know about – therefore they must be constantly updated with signatures of new attacks.
- Many misuse detectors are designed to use tightly defined signatures that prevent them from detecting variants of common attacks. State-based misuse detectors can overcome this limitation, but are not commonly used in commercial IDSs.

- **Anomaly Detection** - Anomaly detectors identify abnormal unusual behavior (anomalies) on a host or network. They function on the assumption that attacks are different from "normal" (legitimate) activity and can therefore be detected by systems that identify these differences. Anomaly detectors construct profiles representing normal behavior of users, hosts, or network connections. These profiles are constructed from historical data collected over a period of normal operation. The detectors then collect event data and use a variety of measures to determine when monitored activity deviates from the norm.

The measures and techniques used in anomaly detection include [14]:

- **Threshold detection,** in which certain attributes of user and system behavior are expressed in terms of counts, with some level established as permissible. Such behavior attributes can include the number of files accessed by a user in a given period of time, the number of failed attempts to login to the system, the amount of CPU utilized by a process, etc. This level can be static or heuristic (*i.e.,* designed to change with actual values observed over time)
- **Statistical measures,** *both parametric,* where the distribution of the profiled attributes is assumed to fit a particular pattern, and *non-parametric*, where the distribution of the profiled attributes is "learned" from a set of historical values, observed over time.
- **Rule-based measures,** which are similar to non-parametric statistical measures in that observed data defines acceptable usage patterns, but differs in that those patterns are specified as rules, not numeric quantities.
- **Other measures,** including neural networks, genetic algorithms, and immune system models. Only the first two measures are used in current commercial IDSs.

Unfortunately, anomaly detectors and the IDSs based on them often produce a large number of false alarms, as normal patterns of user and system behavior can vary wildly. Despite this shortcoming, researchers assert that anomaly-based IDSs are able to detect new attack forms, unlike signature-based IDSs that rely on matching patterns of past attacks. Furthermore, some forms of anomaly detection produce output that can in turn be used as information sources for misuse detectors. For example, a threshold-based anomaly detector can generate a figure representing the "normal" number of files accessed by a particular user. The misuse detector can use this figure as part of a detection signature that says "if the number of files accessed by this user exceeds this "normal" figure by ten percent, trigger an alarm." Although some commercial IDSs include limited forms of anomaly detection, few rely solely on this technology. The anomaly detection that exists in commercial systems usually revolves around detecting network or port scanning. However, anomaly detection remains an active intrusion detection research area and may play a greater part in future IDSs.

Advantages of Anomaly Detection are [14]:

- IDSs based on anomaly detection detect unusual behavior and thus have the ability to detect symptoms of attacks without specific knowledge of details.
- Anomaly detectors can produce information that can in turn be used to define signatures for misuse detectors.

Disadvantages of Anomaly Detection are [14]:

- Anomaly detection approaches usually produce a large number of false alarms due to the unpredictable behaviors of users and networks.
- Anomaly detection approaches often require extensive "training sets" of system event records in order to characterize normal behavior patterns.

3.2.3.1.3 Response Options for Intrusion Detection Systems

Once IDSs have obtained event information and analyzed it to find symptoms of attacks, they generate responses. Some of these responses involve reporting results and findings to a pre-specified location. Others involve more active automated responses. Though researchers are tempted to underrate the importance of good response functions in IDSs, they are actually very important. "Commercial IDSs support a wide range of response options, often categorized as active responses, passive responses, or some mixture of the two." [14]

- **Active Responses** - Active IDS responses are automated actions taken when certain types of intrusions are detected. There are three categories of active responses.

  - **Collect additional information** – "The most innocuous, but at times most productive, active response is to collect additional information about a suspected attack. Each of us have probably done the equivalent of this when awakened by a strange noise at night. The first thing one does in such a situation is to listen more closely, searching for additional information that allows you to decide whether you should take action. In the IDS case, this might involve increasing the level of sensitivity of information sources (for instance, turning up the number of events logged by an operating system audit trail, or increasing the sensitivity of a network monitor to capture all packets, not just those targeting a particular port or target system.) Collecting additional information is helpful for several reasons. The additional information collected can help resolve the detection of the attack (assisting the system in diagnosing whether an attack did or did not take place). This option also allows the organization to gather information that can be used to support investigation and apprehension of the attacker, and to support criminal and civil legal remedies." [14]

- **Change the Environment** – Another active response is to halt an attack in progress and then block subsequent access by the attacker. Typically, IDSs do not have the ability to block a specific person's access, but instead block Internet Protocol (IP) addresses from which the attacker appears to be coming. It is very difficult to block a determined and knowledgeable attacker, but IDSs can often deter expert attackers or stop novice attackers by taking the following actions: [14]
    - Injecting TCP reset packets into the attacker's connection to the victim system, thereby terminating the connection
    - Reconfiguring routers and firewalls to block packets from the attacker's apparent location (IP address or site),
    - Reconfiguring routers and firewalls to block the network ports, protocols, or services being used by an attacker, and
    - In extreme situations, reconfiguring routers and firewalls to sever all connections that use certain network interfaces.

- **Take Action Against the Intruder** – "Some who follow intrusion detection discussions, especially in information warfare circles, believe that the first option in active response is to take action against the intruder. The most aggressive form of this response involves launching attacks against or attempting to actively gain information about the attacker's host or site. However tempting it might be, this response is ill advised. Due to legal ambiguities about civil liability, this option can represent a greater risk than the attack it is intended to block." [14]

The first reason for approaching this option with a great deal of caution is that it may be illegal. Furthermore, as many attackers use false network addresses when attacking systems, it carries with it a high risk of causing damage to innocent Internet sites and users. Finally, strike back can escalate the attack, provoking an attacker who originally intended only to browse a site to take more aggressive action. Should an active intervention and traceback of this sort be warranted (as in the case of a critical system) human control and supervision of the process is advisable. We strongly recommend that you obtain legal advice before pursuing any of these "strike-back" options.

- **Passive Responses** - Passive IDS responses provide information to system users, relying on humans to take subsequent action based on that information. Many commercial IDSs rely solely on passive responses.

  - ♦ **Alarms and Notifications** – "Alarms and notifications are generated by IDSs to inform users when attacks are detected. Most commercial IDSs allow users a great deal of latitude in determining how and when alarms are generated and to whom they are displayed. The most common form of alarm is an onscreen alert or popup window. This is displayed on the IDS console or on other systems as specified by the user during the configuration of the IDS. The information provided in the alarm message varies widely, ranging from a notification that an intrusion has taken place to extremely detailed messages outlining the IP addresses of the source and target of the attack, the specific attack tool used to gain access, and the outcome of the attack. Another set of options that are of utility to large or distributed organizations are those involving remote notification of alarms or alerts. These allow organizations to configure the IDS so that it sends alerts to cellular phones and pagers carried by incident response teams or system security personnel. Some products also offer email as another notification channel. This is ill advised, as attackers often routinely monitor email and might even block the message." [14]

  - ♦ **SNMP Traps and Plug-ins** – "Some commercial IDSs are designed to generate alarms and alerts, reporting them to a network management system. These use SNMP traps and messages to post alarms and alerts to central network management consoles, where they can be serviced by network operations personnel. Several benefits are associated with this reporting scheme, including the ability to adapt the entire network infrastructure to respond to a detected attack, the ability to shift the processing load associated with an active response to a system other than the one being targeted by the attack, and the ability to use common communications channels." [14]

- **Reporting and Archiving Capabilities** - "Many, if not all, commercial IDSs provide capabilities to generate routine reports and other detailed information documents. Some of these can output reports of system events and intrusions detected over a particular reporting period (for example, a week or a month.) Some provide statistics or logs generated by the IDS in formats suitable for inclusion in database systems or for use in report generating." [14]

3.2.3.2 Intrusion Detection System Examples

Some examples of intrusion detection systems and their qualifications will be explained next. These intrusion detection systems are NIDES, Snort and Symantec Intruder Alert.

3.2.3.2.1 Next Generation Intrusion Detection System

Next Generation Intrusion Detection Expert System (NIDES) is a comprehensive intrusion-detection system that performs real-time monitoring of user activity on a set of target system computers and detects unusual and suspicious user behavior in real time on those target systems. NIDES runs on its own workstation and analyzes audit data characterizing user activity collected from monitored systems to detect a variety of suspicious user behavior.

NIDES performs two types of analysis: [15]

- NIDES' statistical analysis maintains historical statistical profiles for each user and raises an alarm when observed activity departs from established patterns of use for an individual. The historical profiles are updated regularly, and older data "aged" out with each profile update, so that NIDES adaptively learns what to expect from each user.

This type of analysis is intended to detect intruders masquerading as legitimate users. Statistical analysis may also detect intruders who exploit previously unknown vulnerabilities who could not be detected by any other means. Statistical anomaly detection can also turn up interesting and unusual events that could lead to security-relevant discoveries upon investigation by a security officer. The statistical analysis is customizable: several parameters and thresholds can be changed from their default values, and specific intrusion-detection "measures" (the aspects of behavior for which statistics are kept) can be turned on or off.

- NIDES' rule-based analysis uses rules that characterize known intrusion types to raise an alarm if observed activity matches any of its encoded rules. This type of analysis is intended to detect attempts to exploit known security vulnerabilities of the monitored systems and intruders who exhibit specific patterns of behavior that are known to be suspicious or in violation of site security policy. Observed activity that matches any of these predefined behaviors is flagged. Unlike most competing systems, the NIDES rulebase is customizable: new rules can be defined and compiled into the running system, and existing rules can be turned on or off. Although NIDES comes with a limited rulebase designed for Sun UNIX operating systems, you will want to customize the rulebase for your particular environment and to keep it up to date with the changing vulnerabilities of new system releases and discovered vulnerabilities of current releases.

"The NIDES resolver screens the alarms generated by the statistical and rulebased components before reporting them to the security officer, to avoid flooding the security officer with redundant alarms." [15] Alerts can be reported to the NIDES console or to a list of email recipients. Some user-configurable filters are also provided. For example, "Alert reporting for specific users can be turned off, if it is known that they will be doing something unusual. Otherwise it will generate a lot of false alarms. Although filtered alerts are not reported, they are still logged." [15]

NIDES includes an archive facility that stores audit records, analysis results, and alerts, and allows browsing of this archive. NIDES also includes a system monitoring facility that displays information on monitored systems, status of the audit data archiver, a daily summary of system throughput, and a daily summary of alert generation.

NIDES also includes a test facility that allows a security officer to experiment with new statistical parameter settings or new rulebase configurations before committing them to the running NIDES. The NIDES user may construct test data sets from the audit record archive for a specific time window and set of user names. The candidate rulebase and statistical parameters can then be tested against these test data sets concurrent with the running NIDES. Test results are archived for comparison.

NIDES can operate either in real time, for continuous monitoring and analysis of user activity, or in batch mode, for periodic batch analysis of audit data. "NIDES can monitor numerous, possibly heterogeneous, machines. The monitored systems provide audit data to NIDES for analysis. process that runs on each monitored system converts audit data in the monitored system's native audit record format to a generic audit data format used by NIDES and (in real-time mode) transmits the NIDES-formatted audit data to NIDES. NIDES receives data from multiple monitored systems and coalesces the data into a single audit record stream for analysis. Because NIDES uses a generic audit record format, it is easily adapted to monitor new system types by writing a simple audit data mapping routine (mapping routines for some system types are already available)." [15]

NIDES includes a user interface written using the MOTIF toolkit to operate under the X-Window system. Access to the various NIDES functions is provided a pulldown menus, point-and-click selections, and occasional text entry. An extensive multitiered context-sensitive help system is included. NIDES also includes a comprehensive user's manual and tutorial.

3.2.3.2.2 Snort

"Snort is a libpcap-based packet sniffer and logger that can be used as a lightweight network intrusion detection system (NIDS)." [16] It features rules based logging to perform content pattern matching and detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and much more. Snort has real-time alerting capability, with alerts being sent to syslog, Server Message Block (SMB) "WinPopup" messages, or a separate "alert" file. Snort is configured using command line switches and optional Berkeley Packet Filter commands. The detection engine is programmed using a simple language that describes per packet tests and actions. Ease of use simplifies and expedites the development of new exploit detection rules. For example, "When the IIS Showcode web exploits were revealed on the Bugtraq mailing list, Snort rules to detect the probes were available within a few hours." [16]

Snort shares commonalities with both sniffers and Network IDSs. Snort decodes the application layer of a packet and can be given rules to collect traffic that has specific data contained within its application layer. This allows Snort to detect many types of hostile activity, including buffer overflows, CGI scans, or any other data in the packet payload that can be characterized in a unique detection fingerprint.

Another Snort advantage is that its decoded output display is user friendly. Snort does not currently lookup host names or port names while running. Snort is focused on collecting packets as quickly as possible and processing them in the Snort detection engine. Performing run-time host name lookup is not conducive to high performance packet analysis.

One feature of Snort is the capability to filter traffic with Berkeley Packet Filter (BPF) commands. "This allows traffic to be collected based upon a variety of specific packet fields." [16] For example, "Both tools may be instructed via BPF commands to process TCP traffic only." [16] Snort can utilize its flexible rules set to perform additional functions, such as searching out and recording only those packets that have their TCP flags set a particular way or containing web requests that amount to CGI vulnerability probes. Snort's architecture is focused on performance, simplicity, and flexibility. There are three primary subsystems that make up Snort [16]:

- The packet decoder,
- The detection engine,
- The logging and alerting subsystem.

These subsystems ride on top of the libpcap promiscuous packet sniffing library, which provides a portable packet sniffing and filtering capability. Program configuration, rules parsing, and data structure generation takes place before the sniffer section is initialized, keeping the amount of per packet processing to the minimum required to achieve the base program functionality.

Snort will run on any platform where libpcap will run. The current version of Snort is 1.2.1, and libpcap is required to compile and run the software. Snort is known to run on RedHat Linux 5.1/5.2/6.0, Debian Linux, MkLinux, S/Linux, HP-UX, Solaris 2.5.1 - 2.7 (x86 and Sparc), x86 Free/Net/OpenBSD, M68k NetBSD, and MacOS X

3.2.3.2.3 Intruder Alert

"Intruder Alert monitors systems and networks in real time to detect and prevent unauthorized activity. It enables the creation of powerful, customizable intrusion detection policies and responses and also policy enforcement with the automatic deployment of new policies and updated detection signatures. Intruder Alert also delivers network-wide responses to security breaches from a central management console." [17]

Symantec Intruder Alert 3.6 is a host-based, real-time intrusion monitoring system that detects unauthorized activity and security breaches and responds automatically. If Intruder Alert detects a threat, an alarm is sounded or other countermeasures are taken according to pre-established security policies in order to prevent information loss or theft. From a central console, administrators can create, update, and deploy policies and securely collect and archive audit logs for incident analysis, all while maintaining the availability and integrity of systems. "As a complement to firewalls and other access controls, Intruder Alert enables the development of precautionary security policies that prevent expert hackers or authorized users with malicious intent from misusing systems, applications, and data. Intruder Alert provides complete control over systems with policy-based management that determines which systems and activities to monitor and what actions to take, as well as with real-time intrusion detection reports for both host and network components. Administrative wizards perform many routine tasks and silent installation and remote tune-up capabilities make it easy to deploy and maintain the system." [17]

Symantec Intruder Alert 3.6 includes specialized software agents that support server platforms running Windows NT, most commercial versions of UNIX, and Novell NetWare. It can also be configured to monitor Web or database applications running on servers.

3.2.3.3 Intrusion Detection Systems and GASSP Principles

Some of the Generally Accepted System Security Principles (GASSP) can be used in developing and using in detection process of attacks and providing alerts to the security administrator of the organizations. The relevant GASSP principles are Timeliness Pervasive Principle, and Accountability Broad Functional Principle. Also a detailed security principle about intrusion detection systems can be formed.

All parts of the organizations measures should act in a timely manner to prevent and avoid the attacks and intrusions to be made to the organization's information system. Intrusion detection systems should detect the intrusions as soon as possible, rise alarms and also try to avoid the attack to give harm to the system. Also management should hold all the parts of the system accountable for their access and use of information. Intrusion detection systems hold the audits of the system and so all the additions, modifications, deletions etc. to the system and their accountable users can be logged and known by the system.

3.2.3.3.1 Developed Detailed Security Principle About Intrusion Detection Systems

The principle can be stated as, *"Use intrusion detection systems in the process of detecting all the potential attacks and intrusions to the system that an attacker is attempting to give harm or to get unauthorized information."* Intrusion detection systems are able to detect the intrusions by auditing the system and matching the audits with known intrusion scenarios and also some types of them with statistical analysis of the audits and user profiles. As seen above intrusion detection systems must used in detecting the intrusions to the systems, which may be dangerous and harmful for the information system.

3.2.4 Integrity Checkers

Integrity checkers resides in the recovery sub-layer of the intrusion management systems and also in the detection sub-layer of intrusion management architecture. File Integrity Checkers are another class of security tools that complement intrusion detection systems. Integrity checking tools detect and notify system administrators of changed, added, or deleted files in some meaningful and useful manner. Integrity analysis focuses on whether some aspect of a file or object has been altered. This often includes file and directory attributes, content and data streams. Integrity analysis often utilizes strong cryptographic mechanisms, called *message digest (*or *hash) algorithms,* which can recognize even subtle changes. They utilize message digest or other cryptographic checksums for critical files and objects, comparing them to reference values, and flagging differences or changes.

The use of cryptographic checksums is important, as attackers often alter system files, at three stages of the attack. "First, they alter system files as the goal of the attack (e.g., Trojan Horse placement), second, they attempt to leave back doors in the system through which they can reenter the system at a later time, and finally, they attempt to cover their tracks so that system owners will be unaware of the attack." [14]

Although File Integrity Checkers are most often used to determine whether attackers have altered system files or executables, they can also help determine whether vendor-supplied bug patches or other desired changes have been applied to system binaries. They are extremely valuable to those conducting a forensic examination of systems that have been attacked, as they allow quick and reliable diagnosis of the footprint of an attack. This enables system managers to optimize the restoration of service after incidents occur.

Any successful attack where files were altered, network packet grabbers were left behind, or root-kits were deployed will be detected regardless of whether or not the attack was detected by signature or statistical analysis.

Because current implementations tend to work in batch mode, they are not conducive to real-time response. And also meaningfully reporting changed files is difficult, because most files are expected to change: system log files are written to, program sources are updated, and documents are revised.

3.2.4.1 Integrity Checker Examples

Some examples integrity checkers and their qualifications will be explained next. These integrity checkers are Tripwire, Samhain, CHECK.

3.2.4.1.1 Tripwire

Tripwire is an integrity checking program written for Unix environments. It has released first in November 2, 1992 by Gene Kim and Dr. Eugene Spafford (of the COAST laboratory at Perdue University) [18]. It is portable, scalable, configurable, and secure. Tripwire is portable because, it is written in standard K&R C, adhering to POSIX standards whenever possible. It can run on [18]:

- NT 4.0
- Solaris (Intel and SPARC) 2.6 and 7.0
- IBM AIX 4.2 and 4.3
- HP-UX 10.20 and 11.0
- SGI IRIX 6.5
- Linux

Tripwire is determined as scalable because it has a preprocessing language. Its configuration and database files can be read from any file descriptors open at the time of Tripwire invocation. It supports UNIX style pipes.

Tripwire's configuration files may be shared between multiple machines. Each entry includes a selection-mask describing which file (inode) attributes can change without being reported. It includes general templates for quick file classification. These are [18]:

- **read-only files** The access timestamp is ignored.
- **log files** Changes to file size, access and modification timestamps, and signatures are ignored.
- **growing log files** Same as log files except only increasing file sizes are ignored
- **ignore nothing** and **ignore everything**

Tripwire is recommends storage of database on read-only media. Database contains on information that could aid an intruder in compromising the integrity checking scheme. The signature spoofing reduced by choice of message digest algorithm. It is self-contained and it may be run without privilege. It reports, but it does not effect changes. Tripwire can be used in applications like [18]:

- Intrusion Detection.
- Damage Assessment and Recovery
- Forensics
- Policy Compliance
- Software Verification.

It includes signature functions of CRC-32, HAVAL, MD5, and SHA.

3.2.4.1.2 Samhain

"Samhain is a file system integrity and intrusion detection tool that allows to trace what changes have occurred on a file system, when these changes have occurred, and who was logged into the system in the respective time." [19]

Samhain is designed for intuitive configuration and tamper-resistance, and can be configured as a client/server application to monitor many hosts on a network from a single central location. Samhain uses a database of file signatures, including a cryptographic checksum, compares the current state of files and directories against this database, identifies changes, and reports on them if a policy violation is detected.

"Samhain can be run as a daemon process, and is designed to leave a recognizable trace if the daemon is stopped and restarted." [19] For networks, samhain can be used as a client/server system with a central log server. Database and configuration files can be stored on the server, and downloaded by clients at startup. Strong authentication is used for client/server TCP/IP connections. For single-host usage, samhain supports logging to a cryptographically signed log file, to e-mail, syslog, and the console. In addition, external scripts may be invoked e.g. for paging. The configuration file and the database can be signed with PGP, and thus do not need to be on write-only media.

For usage on a single host, Samhain can be compiled without client/server code, to produce a smaller executable. To prevent modification of existing records, the local log file entries are signed using a hash chain, with an original key generated at random. The image of the running process only holds the current key. Keys used for signing past entries are lost - they can only be computed if the original key is known. This original key is emailed to the designated recipient, transparently encrypted with a one-time pad. Only someone who has catched the email and has access to the executable may modify the log file. Both the configuration file and database can be signed by PGP/GnuPG to prevent tampering. Alternatively, Samhain can compute the checksums of both and report them, thus allowing verifying their integrity. To be able to trace modifications of the file system even if an intruder has deleted the database, it is probably a good idea to have a secure backup of the database.

"Samhain is a system that has been designed to facilitate secure and easy monitoring of multiple hosts in a network. It consists of monitoring daemon processes running on individual hosts, and (optionally) a central log server collecting reports from these daemons via TCP/IP connections." [19]

Strong authentication is used to prevent uploading of fake messages to the server. With each client, the server will first engage in a protocol for authentication of the client and exchange of a session key. Connections from unregistered hosts are dropped immediately, and connections from registered hosts are dropped if the client cannot successfully complete the authentication protocol. Once the session key is established, the client will use it to sign its messages. On receipt of a message, the server will check the signature of the client, then remove it and add its own signature when writing to the log file.

Both the configuration file and database can be stored centrally on the server side, and downloaded by the client on startup. A rapid deployment system allows fast, secure and easy installation on multiple hosts. To facilitate the construction of a single configuration file for all hosts on the network, samhain allows conditionals based on hostname, machine, and operating system in the configuration file. Conditionals may be nested, negated, and may use regular expressions.

"Samhain can be also compiled with support for a stealth mode of operation, meaning that the program can be run without an obvious trace of its presence on disk." [19] While it is trivial to run a program under a different name, the presence of the program can still be inferred e.g. from the presence of configuration files, or by searching for strings embedded within the executables on disk. Samhain offers the following options [19]:

- printable strings in the executable, and in the log and database files, can obfuscated, such that they look like binary data,
- command-line parsing can be disabled,
- configuration data can be hidden in an image file by steganography (a utility program for steganography is included), and
- the executable can be packed using compression and encryption.

The database and log file may be hidden by appending them to an already existing image. As the image will display normally, and the appended data are at first sight indistinguishable from binary (image) data, some effort would be required to find them.

3.2.4.1.3 Check

"CHECK is a utility which can help detecting viruses. It's not a virus scanner - it will not scan for viruses in the memory or on the disks. It will try to detect suspicious things like modified memory, files, boot records, interrupts, etc. instead." [20]

CHECK tests the integrity of the [20]:

- Master Boot Record
- Partition Tables
- Boot Sectors
- Interrupts
- Memory
- Upper Memory
- BIOS
- CMOS
- Files (CRC and code checks)

CHECK uses CRC algorithms for checksums. It uses the same polynoms as the McAfee VALIDATE and SCANV programs. The data is stored in a text file, so you can view it simply each line in the file consists of the filename, the both checksums and the file size.

It will detect modifications in files. A virus cannot exist without certain instructions. CHECK checks the code of the executables for certain modified / new instructions. This method is not as reliable as the validation, but it's much faster and gives you additional security. Note that this method will discover viruses, but possibly not destroyed or modified data.

CHECK can also check the Master Boot Record of the harddisk. Each physical harddisk has only one MBR. The MBR contains the code to load the boot sector of the active (the bootable) partition and the partition table. There can be more than one partition table on the harddisk if extended partitions have been used. CHECK will save all partition tables.

"If CHECK detects that an executable file was modified, and if it is sure that you this file have not been modified by authorized parties (installing a new version, re-compiling the sources, etc.) deleting the file is recommended." [20] A good virus scanner could recognize and remove the virus (if it's a known virus) but possibly could not be able to restore the file to its original state. It can happen that a scanner thinks to have recognized one virus but the file is infected with a different virus or even a new version of the same virus and this can lead to some serious problems (like, the virus remains in the file). To keep backups of all the files is reasonable for these reasons [20]. Some programs are able to modify itself or other executables - for example to write configuration data, some antivirus programs add data to the files, etc [20].

3.2.4.2 Integrity Checkers and GASSP Principles

Some of the Generally Accepted System Security Principles (GASSP) can be used in developing and using integrity checkers in detection process of attacks, and system integrity checks. The relevant GASSP principle is System Integrity Broad Functional Principle. This principle of GASSP can be used in integrity checking process of the information systems` of an organization. Also a detailed security principle can be formed for integrity checkers.

Management shall ensure that all properties of systems and applications that are essential to or relied upon to support the organization's mission are established, preserved, and safeguarded. To be able to understand if there is an intrusion to the information system an integrity check of the system and files should be made. In this process integrity checkers plays an important role. And in this process System Integrity Broad Functional Process can give a good guidance.

3.2.4.2.1 Developed Detailed Security Principle About Integrity Checkers

The principle can be stated as, *"Use integrity checker programs in the process of checking the integrity of the computer system against changes, adding, or deleting files."* Integrity analysis focuses on whether some aspect of a file or object has been altered. The attacks, which are successful and give harm to the system and files can be revealed by checking the modifications, adding or deleting processes acted on the files. By doing integrity check, attacks to the integrity of the system can be detected and the harms may be recovered. So, integrity checkers may be used in recovery layer of the intrusion management systems.

3.3 Developed Detailed Security Principles In The Thesis Work

The developed detailed security principles about the tools of Intrusion Management Systems are stated in the following subsections. A cross-impact matrix related to developed principles to the pervasive and broad functional principles (Figure 3.1) is also included at the end of this section.

3.3.1 Developed Detailed Security Principle About Firewalls

The principle can be stated as *"Use firewalls in the process of preventing the attacks coming from outside to the organization's information system."* Firewalls are able to prevent the types of attacks, which are possible for an organization's network by denying the connections to the system in regard to their configurations. As seen above firewalls are used in avoidance layer of the intrusion management systems for preventing the system from the attacks. The GASSP principles about this process' point out the firewalls.

3.3.2 Developed Detailed Security Principle About Vulnerability Scanners

The principle can be stated as *"Use vulnerability scanner programs in the process of checking all of the potential methods that an attacker might use to tamper with an organization's network."* Vulnerability scanners are able to determine the types of attacks, which are possible for an organization's network, by analyzing network's software types and software configurations. Both known and unknown vulnerabilities can be checked by many of the vulnerability scanners. As indicated, above vulnerability scanners are used in vulnerability assessment process of the information systems and they play an important role in this process. The GASSP principles about this process' point out the vulnerability scanner tools and vulnerability scanning.

3.3.3 Developed Detailed Security Principle About Intrusion Detection Systems

The principle can be stated as *"Use intrusion detection systems in the process of detecting all the potential attacks and intrusions to the system that an attacker is* *attempting to give harm or to get unauthorized information."* Intrusion detection systems are able to detect the intrusions by auditing the system and matching the audits with known intrusion scenarios and also some types of them with statistical analysis of the audits and user profiles. Intrusion detection systems must used in detecting the intrusions to the systems, which may be dangerous and harmful for the information system.

3.3.4 Developed Detailed Security Principle About Integrity Checkers

The principle can be stated as *"Use integrity checker programs in the process of checking the integrity of the computer system against changes, adding, or deleting files."* Integrity analysis focuses on whether some aspect of a file or object has been altered. The attacks - which are successful and give harm to the system and files - can be revealed by checking the modifications, adding, or deleting processes acted on the files. By doing integrity check, attacks to the integrity of the system can be detected and the loss may be recovered. So, integrity checkers may be used in recovery layer of the intrusion management systems.

3.3.5 Cross Impact Matrix

The following matrix in Figure 3.1 presents the relationship of the Developed Detailed Security Principles (DSP) and the Pervasive (PP) and Broad Functional (BFP) Principles of GASSP. It indicates the GASSP principle that is used in developing the detailed security principles about the tools of Intrusion Management Systems. For example, the Detailed Security Principle about Intrusion Detection Systems is developed by using Timeliness Pervasive Principle (PP-7) and Accountability Broad Functional Principle (BFP-3).

GASSP Principles	DSP for Firewalls	DSP for Vulnerability Scanners	DSP for Intrusion Detection Systems	DSP for Integrity Checkers
PP-1				
PP-2				
PP-3				
PP-4				
PP-5				
PP-6				
PP-7			X	
PP-8		X		
PP-9				
BFP-1				
BFP-2				
BFP-3			X	
BFP-4				
BFP-5				
BFP-6				
BFP-7				X
BFP-8				
BFP-9	X			
BFP-10		X		
BFP-11		X		
BFP-12	X	X		
BFP-13				
BFP-14				

Figure 3.1: Cross-Impact Matrix Relating to DSP's to PP's and BFP's.

CHAPTER 4

CONCLUSION

An Intrusion Management System is a set of integrated tools necessary to avoid intrusions. If avoidance measures taken by the system for intrusions are not successful an intrusion management system is expected to detect the intrusion attempts and intrusions. Moreover, an intrusion management system is responsible for recovering the information system safely to its operating status after an intrusion. Such an intrusion management system can be said successful only if it is truly configured and if it can patch all the vulnerable points of the information system. The security provided by the Intrusion Management Systems should also be reviewed continuously by a security review program. Therefore, a successful security review program for the Intrusion Management Systems must be implemented and developed. To be able to develop such a program, some Detailed Security Principles with the guidance of Generally Accepted System Security Principles (GASSP), have been developed in this thesis work.

Intrusion Management Systems have a four layer architecture. These layers are avoidance, assurance, detection and recovery layers. Each of the tools, which have been examined and for which principles that have been developed, belongs to one of the four layers of Intrusion Management System model. The tools are firewalls for avoidance layer, vulnerability scanners for assurance layer, intrusion detection systems for detection layer and integrity checkers for recovery layer of Intrusion Management systems. Moreover, some commercial examples of these tools have been examined and their qualifications have been explained in the thesis. These tools are Checkpoint Firewall-1, Gauntlet Firewall 6.0, and T-Rex Security Suit for firewalls, eEye Retina, Languard, and Nessus for Vulnerability Scanners, Next Generation Intrusion Detection Expert System (NIDES), Snort and Intruder Alert for intrusion detection systems and Tripwire, Samhain, and Check for Integrity Checker tools.

Principles are the building blocks of standards and procedures and they play an important role in developing standards and procedures. The principles that have been developed in this thesis work can be used as a reference in developing some standards for Intrusion Management System tools. In addition, according to the developed principles in this thesis, new tools can be developed and used in the security review job of Intrusion Management Systems.

The developed principles in this thesis work do not give exact standards and procedures to develop such Intrusion Management System tools, but they give a guidance to the people who want to develop such standards for these tools. The developed principles state which tools can be used in which layer of the Intrusion Management process. Also, the developed principles state that which tool can be used in which process and also the task of this tool in the intrusion management process. Therefore, this thesis work provides a reference to the information security practitioners in the security review job of the Intrusion Management Systems. By using this reference, the avoidance of the intrusions to the information system can be handled more successfully and also the sufficiency of the measures taken can be assured, and also detection of the successful intrusion attempts and recovery of the system can be done better.

Also, as a future work of this thesis work, standards about the tools of Intrusion Management Systems can be developed according to the Detailed Security Principles developed in this thesis work. A computer software, that provides the necessary detailed security principles according to the Generally Accepted System Security Principles can also be developed as a future work as well.

REFERENCES

[1] "NSA Glossary of Terms used in Computer Security and Intrusion Detection" - http://www.sans.org/newlook/resources/glossary.htm, May 20, 2002.

[2] Peter G. Neumann & Donn B. Parker, "A Summary of Computer Misuse Techniques", 12th National Security Conference Baltimore, Maryland October 10-13, 1989.

[3] Peter E. Stephenson, "Intrusion Management: A Top level Model for Securing Information Assets in an Enterprise Environment", EICAR 2000 Best Paper Proceedings

[4] Peter E. Stephenson, "Managing Intrusions", 1998. WEB Address: http://www.imtgroup.com/docs/intrmgmt.htm – Sept 20, 2000

[5] GASSP Committee, "Generally Accepted System Security Principles (GASSP) Version 2.0", June 1999.

[6] Nora Cuppens, "Firewall Limits Presentation", 2002.

[7] Checkpoint, " Firewall-1: A Complete Solution for Securing the Internet", 2001.

[8] PGP (Protecting Your Privacy) Security, "Gauntlet Firewall and VPN", www.pgp.com/products/gauntlet/default.asp - May 09, 2002.

[9] T-Rex Website - http://www.opensourcefirewall.com/trex.html - May 09, 2002.

[10] eEye Retina – www.eeye.com/html/products/retina/retina25.html – Dec. 27, 2001

[11] LANguard – www.gfi.com/languard/security-tools.htm – Dec. 27, 2001

[12] Nessus Web Site– www.nessus.org – December 27, 2001

[13] Rebecca Bace, "An Introduction to Intrusion Detection & Assessment", ICSA 1999.

[14] Rebecca Bace & Peter Bell, " NIST Special Publication to Intrusion Detection Systems", August 16, 2001.

[15] SRI International, "What is NIDES?", http://www.sdl.sri.com/projects/nides/ - May 20, 2002.

[16] Martin Roesch, "Snort - Lightweight Intrusion Detection for Networks" , USENIX LISA '99 Conference, November 1999.

[17] Axent Web Site - www.axent.com - May 20, 2002.

[18] Aaron Mitchell," Tripwire Presentation, Ohio University, ", February 29, 2000.

[19] Samhain – http://samhain.sourceforge.net/surround.html?main_q.html&2 – March 19, 2002.

[20] Vensislav Iliev,"CHECK version 1.5 Manual", 1995.

APPENDIX A

GLOSSARY OF SOME TERMS

Generally Accepted

GASSP are conventional--that is, they become "generally accepted" by agreement (often tacit agreement) rather than formal derivation from a set of postulates or basic concepts. The principles have been developed on the basis of experience, reason, custom, usage, and, to a significant extent, practical necessity. The sources of established information security principles are generally the following [5]:

- Pronouncements of an authoritative body (to be established), as appropriate, to establish information security principles.
- Pronouncements of bodies composed of expert information security practitioners that follow a due process procedure, including broad distribution of proposed information security principles for public comment, for the intended purpose of establishing information security principles or describing existing practices that are generally accepted. This includes information security audit guides and statements of position.
- Practices or pronouncements that are generally accepted because they represent prevalent practice in a particular industry or the knowledgeable application to specific circumstance of pronouncements. This includes interpretations and practices that are widely recognized and prevalent in the industry.
- Other information security literature including pronouncements of other professional associations or regulatory agencies and information security textbooks and articles.

"The concept of generally accepted is to be distinguished from the concept of universally accepted. This distinction is made to address the case that all principles may have exceptions. For example, a library system may insist that the card catalog system have no accountability to preserve the privacy of the user. A process will be provided for use when it is deemed necessary to deviate from the published GASSP." [5]

Generally Accepted System Security Principles (GASSP)

"Generally Accepted System Security Principles" incorporate the consensus, at a particular time, as to the principles, standards, conventions, and mechanisms that information security practitioners should employ, that information processing products should provide, and that information owners should acknowledge to ensure the security of information and information systems.

"GASSP relates to physical, technical and administrative information security and encompasses pervasive, broad functional, and detailed security principles. GASSP nomenclature considers the terms policy, rules, procedures, and practices to relate to the organizational implementation of security. Information technology (IT) changes rapidly, and GASSP are expected to evolve accordingly. Consensus as to accepted information security principles is achieved first within the GASSP Committee followed by international IT community review." [5]

Information

"The term "information" applies to any storage, communication, or receipt of knowledge, such as fact, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any medium." [5]

Information System

"The term "information system" describes the organized collection, processing, transmission, and dissemination or information in accordance with defined procedures, whether automated or manual." [5]

Information Security Principles

The term "information security principles" is used in its broadest context. It includes principles, standards, conventions and mechanisms. Three categories (pervasive, broad functional, and detailed) are used to collect, discuss, and organize security principles. "The broad functional and detailed security principles are divided into principles for information security practitioners and information processing products." [5]

"GASSP will support information security professional certification, information security audit, and information technology product development from an information security perspective. GASSP will also provide authoritative guidance to the information security practitioners, enabling them to establish and maintain their credibility with management" [5]

System

"The term "system" is used as an umbrella term for the hardware, software, physical, administrative, and organizational issues that need to be considered when addressing the security of an organization's information resources. It implies that the GASSP address the broadest definition of information security. The term System is intended to be equivalent in scope of the terms Information Technology (IT), Automated Information System (AIS), Automated Data Processing Element (ADPE), etc." [5]

Activity

"Instantiations of the data source that are identified by the analyzer as being of interest to the security administrator. Examples of this include (but are not limited to) network sessions, user activity, and application events. Activity can range from extremely serious occurrences (such as an unequivocally malicious attack) to less serious occurrences (such as unusual user activity that's worth a further look)." [13]

Agent

"The Intrusion Detection component that periodically collects data from the data source, sometimes performing some analysis or organization of the data. Also known as *sensor.* " [13]

Analyzer

"The Intrusion Detection component that analyzes the data collected by the sensor for signs of unauthorized or undesired activity or for events that might be of interest to the security administrator." [13]

Audit Log

"The log of system events and activities generated by the operating system." [13]

Data Source

"The raw information that an intrusion detection system uses to detect unauthorized or undesired activity. Common data sources include (but are not limited to) raw network packets, operating system audit logs, application audit logs, and system-generated checksum data." [13]

Event

"A notification from an analyzer to the security administrator a signature has triggered. An event typically contains information about the activity that triggered the signature, as well as the specifics of the occurrence." [13]

File Assessment

"A technology in which message digest hashing algorithms are used to render files and directories tamper evident." [13]

Incident Handling

"The part of the Security Management Process concerning the investigation and resolution of security incidents that occur and are detected. Also known as *incident response."* [13]

Intrusion Detection

"The technology concerned with monitoring computer systems in order to recognize signs of intrusions or policy violations." [13]

Manager

"The Intrusion Detection component from which the security administrator manages the various components of the ID system. Management functions typically include (but are not limited to) sensor configuration, analyzer configuration, event notification management, data consolidation, and reporting." [13]

Message Digest Algorithms

"Specialized cryptographic algorithms that are used to render files tamper-evident. The nature of message digest algorithms dictates that if an input data file is changed in any way, the checksum that is calculated from that data file value calculated will change. Furthermore, a small change in the input data file will result in a large difference in the result." [13]

Response

"The actions that an analyzer takes when a signature is triggered. Sending an event notification to the security administrator is a very common response. Other responses include (but are not limited to) logging the activity, recording the raw data (from the data source) that caused the signature to trigger, terminating a network, user, or application session, or altering network or system access controls." [13]

Scanning

"The technology concerned with scanning computer systems and networks in order to find security vulnerabilities. Also known as *vulnerability assessment.* " [13]

Security Administrator

"The human with responsibility for the successful deployment and operation of the intrusion detection system. This person may ultimately charged with responsibility for the defense of the network. In some organizations, the security administrator is associated with the network or systems administration groups. In other organizations. it's an independent position." [13]

Sensor

"The Intrusion Detection component that periodically collects data from the data source. Also known as *agent.* " [13]

Signature

"A rule used by the analyzer to identify interesting activity to the security administrator. Signatures are the mechanism by which ID systems detect intrusions." [13]

System Log

"The log of system events and activities, generated by a system process. The system log is typically at a greater degree of abstraction than the operating system audit log." [13]

Vulnerability Assessment

"The technology concerned with scanning computer systems and networks in order to find security vulnerabilities. Also known as *scanning.*" [13]