IS (INFORMATION SYSTEM) SECURITY OF AN ORGANIZATION AND AN APPLICATION

KURUM VE KURULUŞLARIN BİLGİ SİSTEMİ GÜVENLİĞİ VE BİR UYGULAMA

HAKAN TAN

In partial fulfillment of the
Degree of Master of Science in
Computer Engineering

2011

Institute of Science and Engineering;

This thesis has been approved in partial fulfillment of the requirements for the degree of **MASTER OF SCIENCE IN COMPUTER ENGINEERING** by the committee members.

Chairman (Supervisor) : Prof. Dr. Ziya Aktaş

Member : Doç. Dr Hasan Oğul

Member : Dr. Atilla Özgit

APPROVAL

This thesis is approved by the committee members on 25/01/2011

..../..../2011

Prof.Dr. Emin AKATA

DIRECTOR, INSTITUTE OF
SCIENCE AND ENGINEERING

ACKNOWLEDGEMENTS

I would like to thank my thesis supervisor Professor Ziya Aktaş for his guidance and criticism throughout the completion of this study.

I would also like to express my gratitude to Kerem Ateş and all my colleagues at Barikat Internet Security for their support, understanding and for being my second family.

Finally many thanks to my beloved wife Rengin Saliha Tan for her boundless patience and support to my long work hours during this study.

ÖZ

KURUM VE KURULUŞLARIN BİLGİ SİSTEMİ GÜVENLİĞİ VE BİR UYGULAMA

Hakan Tan
Başkent Üniversitesi Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı

Bu tez çalışmasında kurum ve kuruluşların bilgi sistemi güvenliği konusu ele alınmıştır. Internet kullanımı ve bilgi sistemlerine dayalı iş modellerinin artışı ile bilgi sistemi güvenliği önemli bir hale gelmiştir. Temel güvenlik kavramları ile kurumsal bilgi sistemleri güvenliği konuları ele alınmıştır. Bir güvenlik mimarisi önerebilmek için bir uygulama geliştirilmiştir.

Bu uygulamada sanal bir organizasyon tanımlanmış ve değişiklikler yapılarak güvenli bir mimariye getirilmiştir. Kurum ve kuruluşlarda sıkça kullanılan güvenlik ürünleri değiştirilen yapı ile “defense in depth” stratejisi uygulanarak bütünleştirilmiştir. Bu sayede saldırgan ve varlık arasına birden fazla savunma noktası konulmuştur. Uygulama sonunda ortaya çıkan mimarinin katmanlı yapısı örnek saldırı vektörleri ile test edilmiştir.

ANAHTAR SÖZCÜKLER: bilgi sistemleri, bilgi sistemleri güvenliği, ağ güvenliği, sistem güvenliği, güvenlik mimarisi.

Danışman: Prof.Dr. A. Ziya AKTAŞ, Başkent Üniversitesi, Bilgisayar Mühendisliği Bölümü.

ABSTRACT

IS (INFORMATION SYSTEM) SECURITY OF AN ORGANIZATION AND AN APPLICATION

Hakan Tan
Başkent University Graduate School of Natural and Applied Sciences
Computer Engineering

Security of IS's is a growing concern due to the increased use of internet and information system depended business models. Fundamental security concepts and enterprise IS security subjects are reviewed first in the study. An application is developed in order to propose an architecture of security. In the application, a fictitious organization is defined and modified to reach a secure architecture. Commonly used security products are integrated to the modified architecture with a defense in depth strategy. By this, more than one defense points are established between the attacker and the asset. Resulting architecture is tested against sample attack vectors.

KEYWORDS: information systems, IS security, network security, system security, security architecture.
Advisor: Prof. A. Ziya AKTAŞ, Başkent University, Computer Engineering.

TABLE OF CONTENTS

LIST OF FIGURES

Page

LIST OF TABLES

LIST OF ABBREVIATIONS

COTS	Commercial of-the-shelf
CVSS	Common vulnerability scoring system
DDOS	Distributed denial of service
DLP	Data loss prevention
DMZ	Demilitarized zone
DNS	Domain name system
DOS	Denial of service
FIPS	Federal information processing standards
IDS	Intrusion detection system
IPS	Intrusion prevention system
IS	Information system
IT	Information technology
NAC	Network access control
NAT	Network address translation
NIST	National Institutes of Standards and Technology
SIEM	Security information event management
SOA	Service oriented architecture
SQL	Structured query language
UTM	Unified threat management
VOIP	Voice over internet protocol
VPN	Virtual private networking
SMTP	Simple mail transfer protocol
SSL	Secure sockets layer

1. INTRODUCTION

1.1 Statement of the Problem

Number of information systems that rely on internet increase every day. Many organizations receive support from their IS to provide services based on data stored on computers. Due to its nature internet is an untrusted network. Information Systems are open to internet and therefore, security of information systems is a growing concern. When Russia attacked Georgia in August 2008, simultaneous cyber attacks were performed by Russian civilians to Georgian government and media web sites. This was not the first coordinated attacks of Russians. In April 27, 2007 they have attacked Estonia's government web sites. Although Russian Government denied their involvement, recent incidents at Georgia and Estonia show clues for cyber-attacks and network infiltrations that are carried by nation-states or governments. Considering such global incidents further security needs emerged globally. McAfee [1].

As a result of technological improvements in computer engineering, new ways to share information have been developed. Client-Server software, web applications, voice over IP (VoIP)[1] and much more new information sharing systems bring vulnerabilities that can be exploited to harm individuals and organizations. In order to meet the requirements of new protocols and applications infrastructure of organizations and internet need to be improved. Wireless communication systems are now everyware. Increasing bandwidth of internet enables much more information that can be sent from it and many more other advancements bring new threats. Each new technology has its own properties and challenges to overcome and secure them. Security of information systems are evolving day by day because of this fact.

[1] VoIP; is a general term for a family of transmission technologies for delivery of voice communications over IP networks

In order to satisfy security needs of organizations, amount of resources that are being spent and work done are at the highest level during these days and if we look to the near future it is not hard to guess that the trend will be increasing rapidly. As an example, note that until a near past a simple firewall was enough to secure a system to a certain degree. But now attacks became very sophisticated. Simply limiting access to some services by a firewall is not enough anymore because new attacks use legitimate services that are already open and must remain opened on firewalls. As a result, extra security measures should be used to support others.

Besides such external threat, every day storage capacity of portable drives increase and stealing information thus becomes very easy. Today an employee can copy the organizations 100 gigabyte database to a usb storage drive that has a size of a finger. Because of that, many government and private organizations that have sensitive information had to establish security measures to prevent data leakages. This is relatively a simple issue considering the employees that intend any harm inside and strangers that plan to attack from inside the organizations.

Such examples show that security of information systems should not be taken lightly and it is a broad subject covering all areas of information technologies and fundamental security concepts. Because of that, securing an information system involves definition of the system and architecture of the solution. Though all IS's vary in some way, they also have very much in common. In this study, therefore, typical architecture of an organization will be given according to the most common attributes of organizations and an application is designed on a fictitious organization to demonstrate security issues.

1.2 Previous Work

In this fast paced and detailed field many publications have been produced in order to establish fundamental knowledge of security and to address specific problems and areas. Some publications deal with the problem from a wide perspective and giving less detail and some publications focus on specific fields of

Information systems and give in depth knowledge about how to secure them accordingly.

Vacca [2] includes all aspects of security in his book but not deals with all the details. In his book, he gathered topics covering System Security, Network and Infrastructure Security, Cryptography, Physical Security and Risk Management.

Harrington [3] focuses more on system security. He gives some practical information about how modern Information System infrastructures work. He advocates that in securing IS infrastructures a directional approach is taken. Harrington based his understanding from an outside to inside direction such as securing internet based threats and after the securing local area networks.

Wong and Yeung [4] aim to promote network infrastructure security by describing the vulnerabilities of some network infrastructure devices, particularly switches and routers.

Tipton and Krause [5] encompass a broad spectrum of areas, ranging from the fundamentals of access control, malicious software, and network security to more esoteric, but equally important, organizational culture and governance framework discussions. Lacey [6] deals a different field of security : the human factor. Rather than technologies he gives details about the human side of the field. This includes the users, management, security staff and building security systems that works. His book gives ideas and recommendation related to the human element of Information Systems.

Kanneganti and Chodavarapu [7] feel the urge to write a book about security of service oriented architectures when working on a SOA project for a customer. Their study focuses on intersection of SOA and Security fields that provide comprehensive information about how to build secure SOA applications. According to them securing SOA is not securing an application but securing architecture because SOA is build up from organized internal and external applications in an enterprise.

1.3 Objective of the Study

Objective of this study is to specify security needs of information systems of a typical organization. In order to clarify such needs, a typical security architecture is developed in the thesis. Considering the wide spectrum of the topic, in the thesis technical details of every subject are not given; instead a higher level of view, that is a logical view, is aimed. Hence, organizations that are considering security designs can benefit from the result of this study as a first step of a guidance.

1.4 Organization of the Study

In this study, after an introduction, basic concepts of Information systems and security concepts are discussed. Next, recommendations for governmental information systems are given. Infrastructural security products are given to note available technologies. In later chapters security risk management and design for security topics will be given in detail.

In developing an architecture of security, one needs a sample organization. It may, however, be harmful to use an actual organization as a sample for security architecture development. Therefore, first a fictitious organization is defined in the thesis. Security architecture of such an organization is then developed in the thesis as a case study.

2. BASIC CONCEPTS OF INFORMATION SYSTEMS (IS)

2.1 Definition of a System and Information

In order to define Information Systems it is proper to first define terms Information and System. When making the definition of information, other related terms come to mind like data and knowledge that they are commonly used for one another. Clearing the confusion and to distinguish between them needs to refer to another term: message as noted by Aktaş[8].

Message is a group of characters that are stored, produced and transmitted in the information systems. In other word data or information is stored, produced and transmitted by messages. The content of a message has different levels of meaning depending on whether the message is carrying data, information or knowledge. Level of meaning in messages increases by the order of data, information and knowledge Aktaş[8].

Using such a differentiator, data are groups of characters recognized as having the lowest level of meaning. They are facts and opinions. Information has more meaning than data in that it is useful in present decision situation. Knowledge has the highest level of meaning because it represents information that can be potentially useful in the future decision situations. There is still difficulty in distinguishing terms data, information and knowledge, because certain data element may be information to one user at one time and knowledge to him at a different time or place. Therefore, the use of the term data, information or knowledge in this text is a general term without differentiating the meaning level Aktaş[8].

A system may be defined as a set of interrelated components with a clearly defined boundary, working together to achieve a common set of goals. A system must have elements, environment, interaction between the elements with the environment and most of important of all, goals to be fulfilled. By this definition systems can be made up of other systems as elements to produce bigger systems. And systems are classified broadly into two categories, Natural Systems and Fabricated Systems. Natural Systems include human body, solar system, and others that have not been created by people. In contrast to natural systems fabricated systems are created by people to satisfy some purpose that they have. Because of this nature fabricated systems should serve you, as noted by Obrien and Marakas [9].

2.2 Information Systems

As shown in Figure 2.1, an Information System can be any organized combination of people, hardware, software, communications networks, data resources and policies and procedures that stores, retrieves, transforms and disseminates information in an organization.

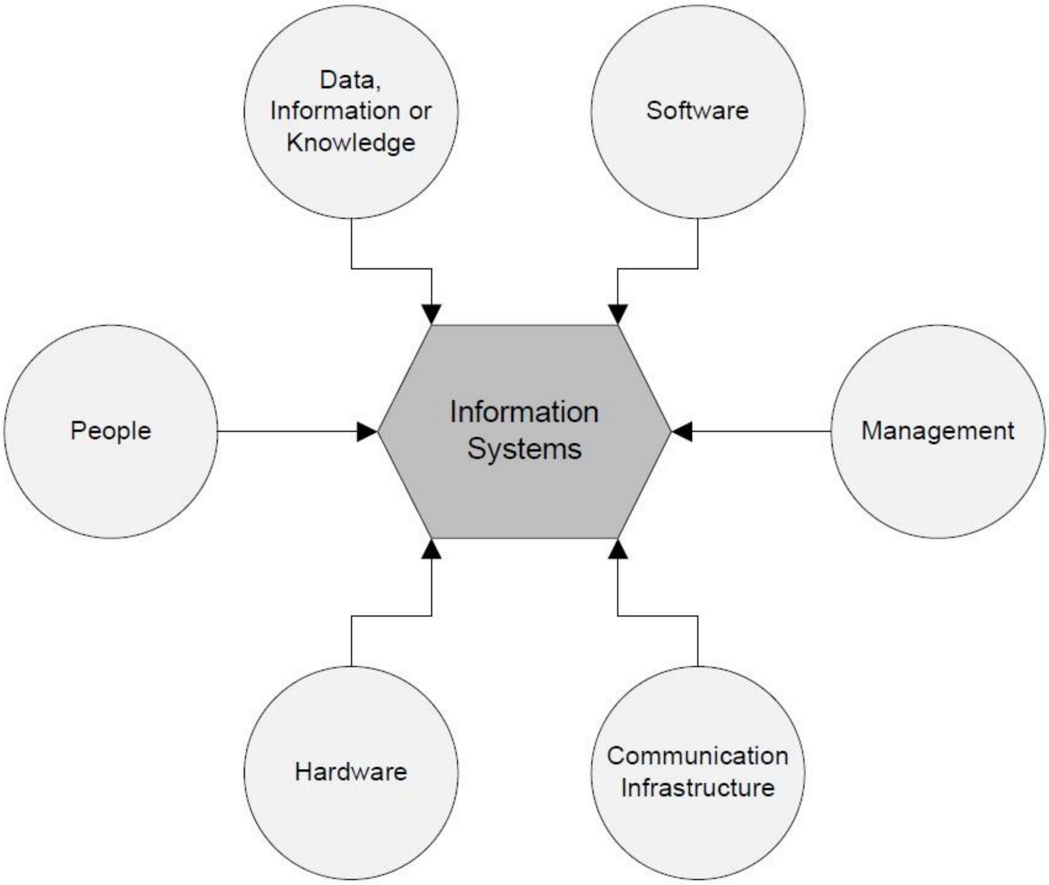


Figure 2.1 Information system components

According to their functions, information systems have three basic activities; input processing and output. Their interaction with the surrounding can be shown in Figure 2.2, as given by Laudon and Laudon [10].

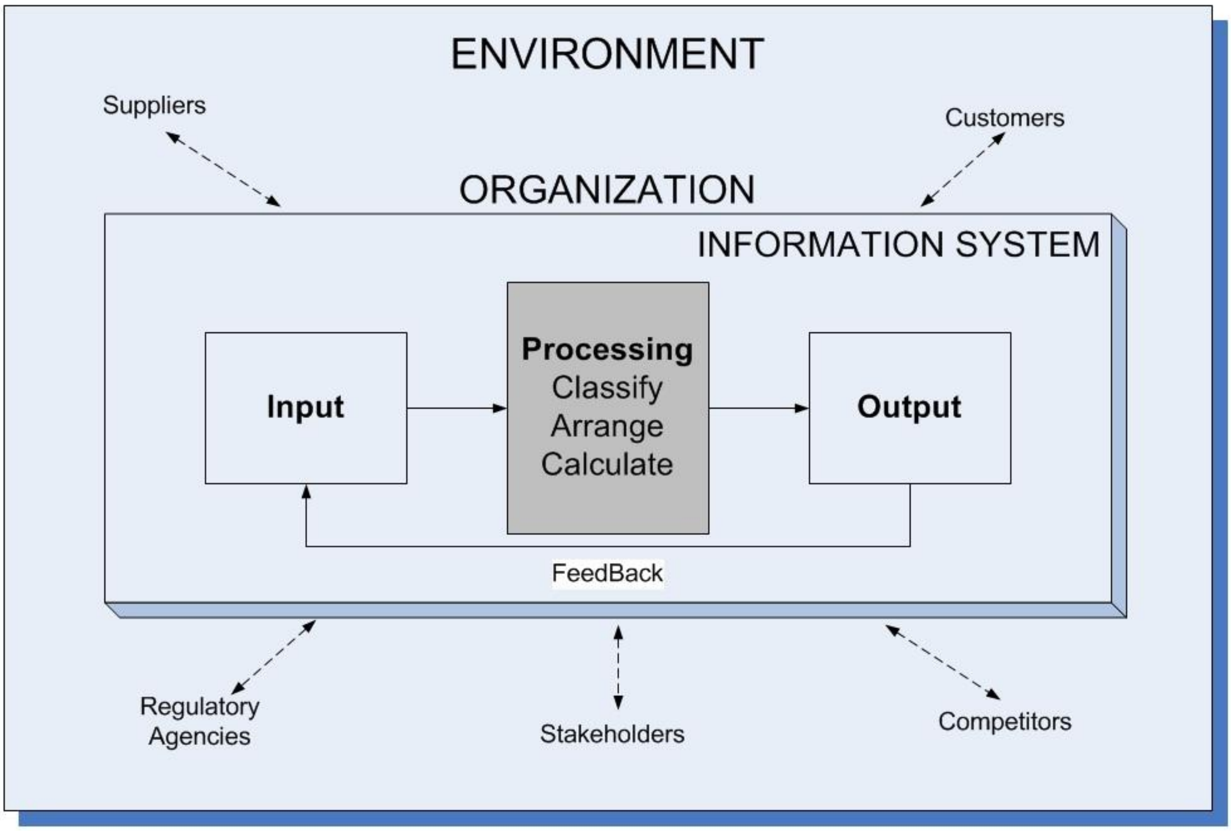


Figure 2.2 Information system of an organization.

Slightly differently Figure 2.3 shows the main components of an information system. All information systems make use of the shown components to perform input, process, output, storage and control activities. O'Brien and Marakas [9].

Information Systems come in all shapes and sizes. They are so interwoven into the fabric of the business systems they support that it is often difficult to distinguish between business systems and their support information systems.

As noted by Bentley and Whitten[11] Information systems can be classified according to the functions of that they serve:

- **Transaction Processing Systems** They process business transactions such as orders, time cards, payments and reservations
- **Management Information Systems** They use the transaction data to produce information needed by managers to run the business.
- **Decision Support Systems** They help various decision makers indentify and choose options and decisions.

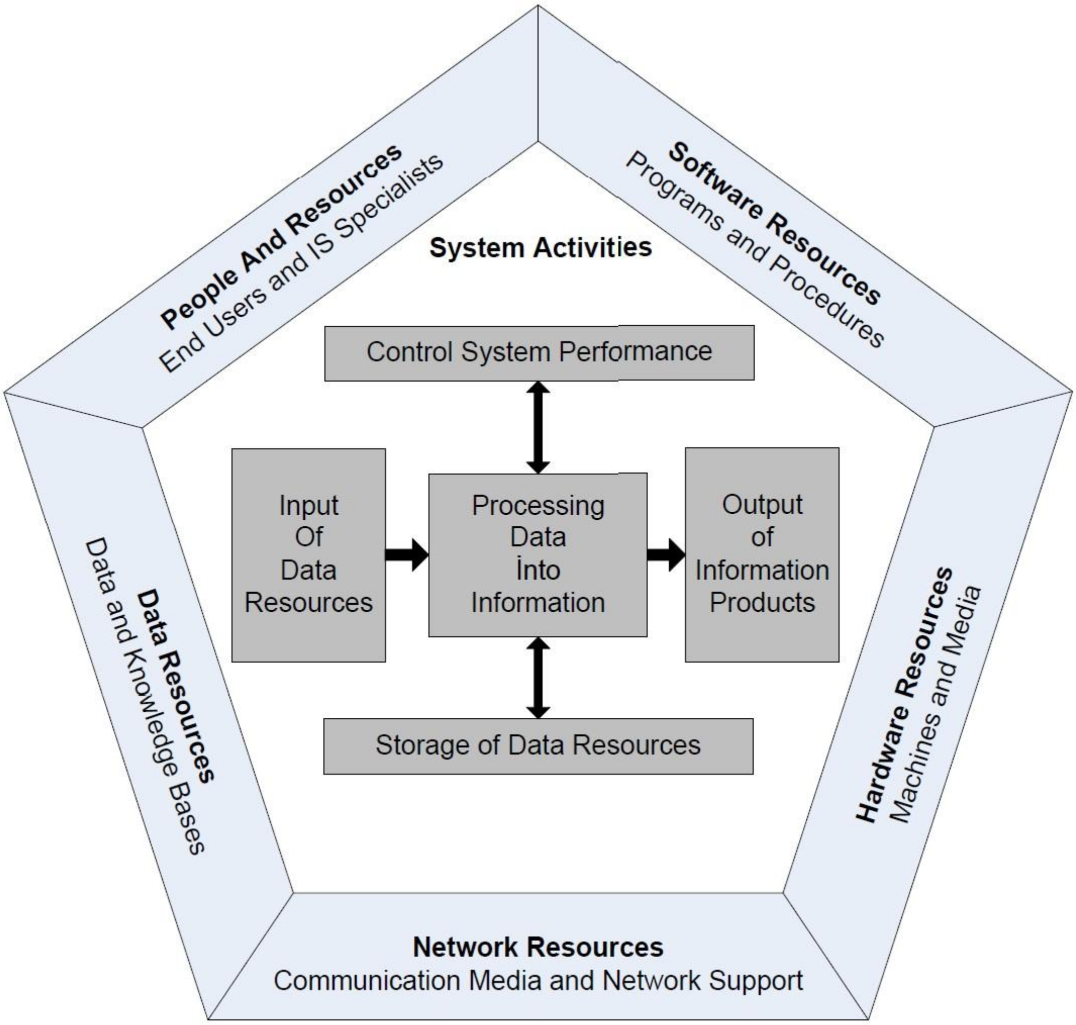


Figure 2.3 An alternative information system

- **Executive Information Systems**: They are tailored to the unique information needs of executives who plan for the business and assess performance against those plans.
- **Expert Systems**: They capture and reproduce the knowledge of an expert problem solver or decision maker and then simulate the thinking of that expert.
- **Communication and Collaboration Systems**: They enhance communication and collaboration between people both internal and external to the organization.
- **Office Automation Systems**: They help employees create and share documents that support day to day office activities.

2.3 Information System Survivability

The system procurer and developer have control over all aspects of the information system that might be attacked. In reality, modern distributed systems inevitably rely on reusable and commercial of-the-shelf (COTS)[2] components which may have been developed separately. Their security characteristics may be external web services and network infrastructures that are outside the control of the application.

This means that irrespective of how much attention is paid to security, it can’t be guaranteed that a system will resist external attacks. Consequently for complex networked systems, penetration is possible and that the integrity of the system cannot be guaranteed. One should therefore think about how to make systems resilient so that it survives to deliver essential services to users even a security failure occurs.

[2] COTS; Commercially available software designed for specific purpose that can be used with little or no modification.

Survivability is an emergent property of a system as a whole rather than a property of individual components, which may not themselves be survivable. The survivability of a system reflects its ability to continue to deliver essential business or mission critical services to legitimate users while it is under attack or after part of the system has been damaged as a consequence of either an attack or system failure, as noted by Sommerville[12].

3. SECURITY CONCEPTS

3.1 Security Engineering

Some of the materials in this chapter are based on Sommerville[12].

The widespread use of the internet in 1990's introduced a new challenge for software engineers, such as designing and implementing systems that were secure. As more and more systems were connected to the Internet, a variety of different external attacks were devised to threaten these systems. The problems of producing dependable systems were hugely increased. Software and Computer engineers had to consider threats from malicious and technically skilled attackers as well as problems resulting from accidental mistakes in the development process.

It is now essential to design systems to withstand external attacks and to recover from these attacks. Without security precautions, it is almost inevitable that attackers will compromise a networked system. They may misuse the system hardware, steal confidential data or disrupt the services offered by the system. System security engineering is therefore an increasingly important aspect of the software and computer engineering process. Security engineering is concerned with how to develop and maintain systems that can resist malicious attacks intended to damage computer-base systems or its data. Security engineering is part of the more general field of computer security, this has become a priority for businesses and individuals as more and more criminals try to exploit networked systems for illegal purposes. Software engineers should be aware of the security threats faced by systems and ways in which these threats can be neutralized.

Vacca[2] claims that there are three distinguished elements of IS security: logical security, physical security, and premises security.

- **Logical security** is protecting computer based data from communication based threats.
- **Physical Security** is protection of physical infrastructure that houses IS.
- **Premises Security** is protection of the physical facilities.

Computer security is a vast field and related to many business and technical aspects of computer engineering. For that reason this thesis focuses especially on the Logical Security which protects IS from software based and communication based threats. Physical security and Premises security can be considered as one.

When considering logical security issues, one have to consider both the application software (the control system, the information system, etc.) and the infrastructure on which this system is built. As given in Figure 3.1 by Sommerville[12] , the infrastructure for complex applications includes an operating system platform, such as Linux or Windows, other generic applications that run on that systems, such as web browsers and e-mail clients, a database management system, middleware that support distributed computing and database access and libraries of reusable components that are used by the application software. In fact, the majority of attacks focus on system infrastructures because the components (e.g. Web Browsers) are well known and widely available.

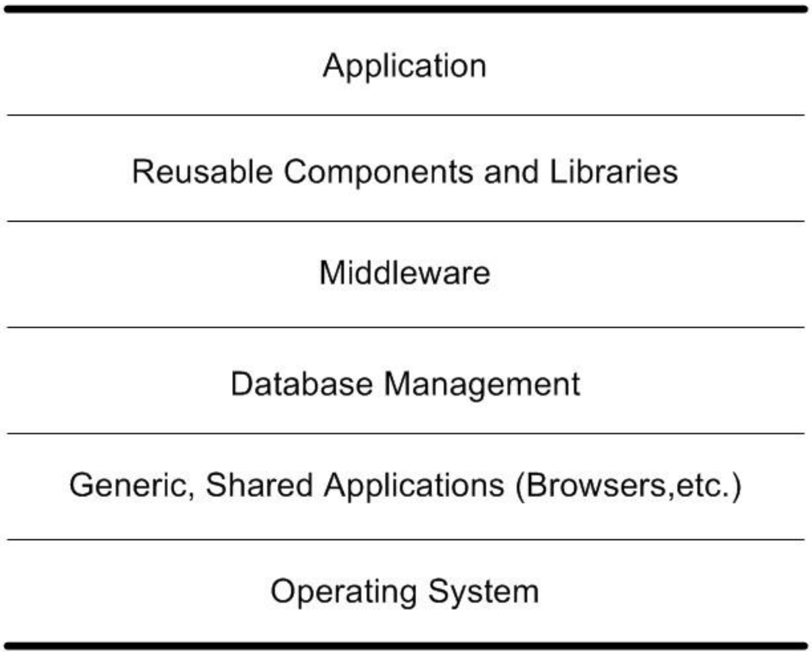

Application
Reusable Components and Libraries
Middleware
Database Management
Generic, Shared Applications (Browsers,etc.)
Operating System

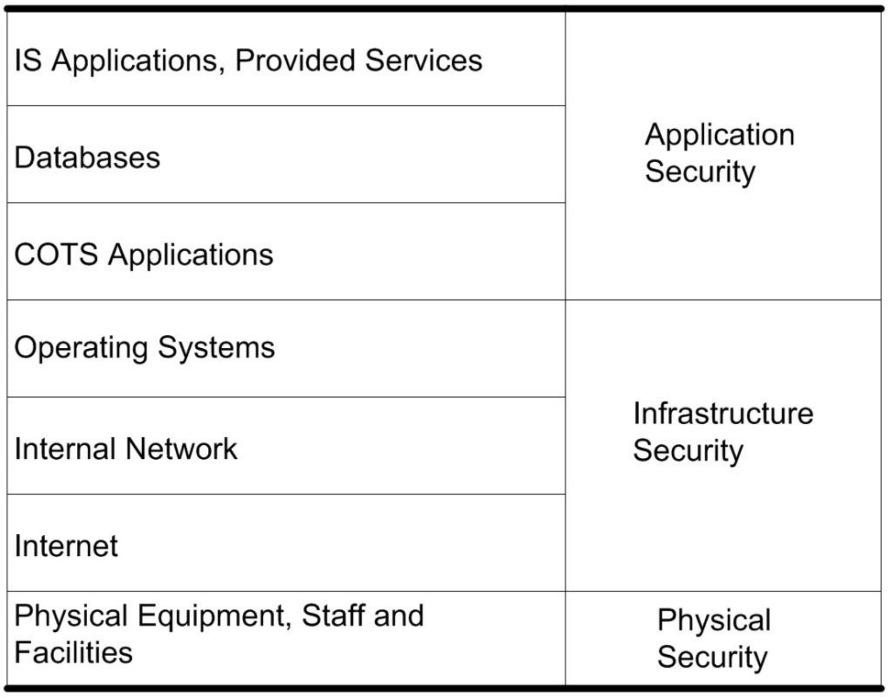
Figure 3.1 Security wise information system layers

In practice, there is an important distinction between application security and infrastructure security:

1. **Application Security** is a software engineering problem where software engineers should ensure that the system is designed to resist attacks.
2. **Infrastructure Security** is a systems management problem where system managers should ensure that the infrastructure is configured to resist attacks. System managers have to setup the infrastructure to make the most effective use of whatever infrastructure security features are available. They also have to repair infrastructure security vulnerabilities that have come to light as the software is used.

As mentioned before, this study focuses on infrastructure security category of logical security rather than the whole computer security field. This doesn’t mean that overall security measures are considered separately. Some infrastructure security precautions such as database or web application security close the security gap that may be introduced by weak or wrong software design. By this idea, infrastructure security precautions should be implemented according to the software systems that are used in an organization.

Sommerville[12] approaches IS security from a software architect/developer point of view. But considering security of IS in an organization, wider point of view must be considered. In his demonstration of IS, some essential layers are absent such as human factor, and detailed infrastructure layers. To establish a more generalized approach, IS layers of an organization are given in Figure 3.2 , with a dependency relationship between levels. Every level generally depends to the layer below. There are also exceptions to this relationship such as operating systems can be used without a network connection or some networks are not exposed to internet in any way. The goal of this idea is to obtain a widely applied state of IS in an organization.



IS Applications, Provided Services	Application Security
Databases	
COTS Applications	
Operating Systems	Infrastructure Security
Internal Network	
Internet	
Physical Equipment, Staff and Facilities	Physical Security

Figure 3.2 Detailed layers of IS of an organization

3.2 Basic Terminology in Security Engineering

A few of the security concepts and terminology that will be used in the thesis are given below: (Vacca [2])

Access: a specific type of interaction between a subject and an object results a information flow.

Asset: anything that has value to the organization, its business operations and their continuity, including information resources that support the organization's mission.

Denial of Service: is prevention of authorized access to or delaying time-critical operations.

Encryption: is the conversion of plaintext or data into unintelligible form by means of reversible translation.

Hacker: is the common nickname for an unauthorized person who breaks into or attempt to break into information systems.

Risk: is the probability that a particular threat will exploit a vulnerability of the system.

Vulnerability: is a weakness of an asset that can be exploited to cause harm.

Attack: An exploitation of a vulnerability that an asset has.

Threats: is the potential that given threat will successfully exploit vulnerabilities of an asset to cause harm to the organization.

As shown in Figure 3.3 referring to Charles[13], Security threats fall to in three principal attributes of IS:

1. Threats to the confidentiality of the system and its data. These can disclose information to people or programs that are not authorized to have access to that information.
2. Threats to the integrity of the system and its data. These threats can damage and corrupt the software or its data.
3. Threats to the availability of the system and its data. These threats can restrict access to the software or its data for authorized users.

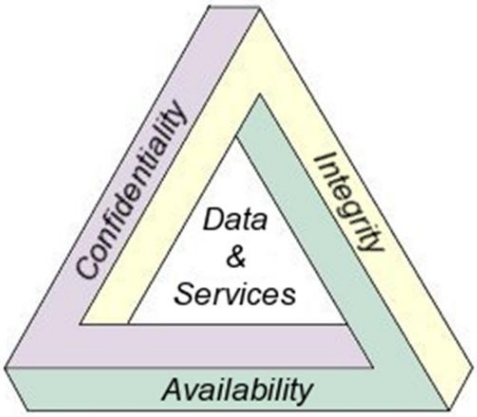


Figure 3.3 The CIA triad

These attributes are, interdependent. If an attack makes the system unavailable, then it will not be updated with information that changes with time. This means that the integrity of the system may be compromised, and then it may have to be taken down to repair the problem. Therefore, the availability of the system is reduced.

3.3 Security Controls

A protective measure that reduces a system's vulnerability or to repel an attack is a security control. Simply, security controls are smallest building blocks or functions to achieve security goals. For example applying least privilege access model is a security control to prevent unnecessary access to assets.

There are alternative ways to categorize security controls. One way is to categorize them on what the control does. If controls are categorized this way they will fall into following three classes as noted by Sommerville[12] :

1. Controls that are preventive, that tries to ensure that attacks are unsuccessful. The strategy here is to design the system so that security problems are avoided. For example, sensitive military systems are not connected to public networks so that external access is impossible. Encryption can be considered as a control base avoidance. Any unauthorized access to encrypted data means that it cannot be read by the attacker. In practice, it is very expensive and time consuming to crack strong encryption.
2. Controls that are intended to detect and repel attacks. These controls involve including functionality in a system that monitors its operations and checks for unusual patterns for activity. If these are detected, then action may be taken, such as shutting down parts of the system, restricting access to certain users, etc.
3. Controls that support recovery from problems. These can range from automated backup strategies and information mirroring through to if the recovery is depended on money, insurance policies that cover costs associated with a successful attack on the system.

It is challenging in deciding which class a particular security control falls into, because most of the time control action can change with the situation. For instance, a security guard can be classified as a preventive control but if an attacker actually attacks, guards can see the attacker and catch him, which makes the control detective and corrective. To avoid this type of confusion, in this study security control categorization mentioned will be according to who does the control rather than what the control does. NIST [14] uses this approach and organized security controls as classes and families for ease of use in the control selection and specification processes for information system applications in an organization. Families together make up general classes of security controls.

The main classes are:

- Technical Controls
- Operational Controls
- Management Controls

According to such categorization, example of security guards belong to access control family and access control family belongs to technical controls.

Simply, management controls are techniques that are normally addressed by management in the organizations IT security program.

Technical controls emphasize the security controls that the computer system executes. As opposed to technical controls, operational controls are those controls that are enforced by people.

There are 17 families under the main three classes and their list is given in the Table 3.1 as given by NIST [14].

In order to achieve a good security posture, these three main classes of security controls should be applied to software systems that are developed within the organization and must be evaluated on the purchased security software and other software that is used in the organization. It should not be missed that any system is strong as its weakest component. Therefore selected security controls should not be focused on a particular class, all needed technical, operational and management controls should be applied to reach desired amount of security.

Table 3.1 Security control classes and families.

CLASS	FAMLIY	EXAMPLE SECURITY CONTROLS
Management	Certification, Accreditation, and Security Assessments	• Security Assessments • IS connections • Security Certification
	Planning	• System security plan • Rules of Behavior • Security related activity planning
	Risk Assessment	• Security categorization • Risk assessment • Vulnerability scanning
	System and Services Acquisition	• Allocation of resources • Life cycle support • Software usage restrictions
Operational	Awareness and Training	• Security Awareness • Security Training • Security Training Records
	Configuration Management	• Baseline Configuration • Configuration change control • Access restriction for change
	Contingency Planning	• Contingency Plan • Contingency Training
	Incident Response	• Incident response training • Incident response training and exercises • Incident Handling
	Maintenance	• Controlled Maintenance • Maintenance tools
	Media Protection	• Media Access • Media Labeling • Media Sanitization
	Personnel Security	• Position categorization • Personnel screening • Personnel termination
	Physical and Environmental Protection	• Physical Access Authorizations • Monitoring Physical Access • Visitor control
	System and Information Integrity	• Flaw remediation • Malicious code protection • Information system monitoring tools and techniques

Table 3.1 (Continued)

Technical	Access Control	• Access control policy and procedures • Account Management • Remote Access
	Audit and Accountability	• Audit and Accountability Policy and Procedures • Audit Monitoring, Analysis and Reporting • Time Stamps
	Identification and Authentication	• User identification and authentication • Device identification and authentication • Identifier Management
	System and Communications Protection	• Application partitioning • Security function isolation • Denial of service protection

4. A SECURITY SYSTEM RECOMMENDATION FOR GOVERNMENTAL INFORMATION SYSTEMS

4.1 General

Security related recommendations and standards for federal information systems of the US are given by NIST[14] , [15]. In this chapter they are summarized.

“The selection and employment of appropriate security controls for an information system are important tasks that can have major implications on the operations and assets of the organization as well as the welfare of individuals. Security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. There are several important questions that should be answered by organizational officials when addressing the security considerations for their information systems as noted by NIST [15]:

- What security controls are needed to adequately protect the information systems that support the operations and assets of the organization in order for that organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals?
- Have the selected security controls been implemented or is there a realistic plan for their implementation?
- What is the desired or required level of assurance (i.e., grounds for confidence) that the selected security controls, as implemented, are effective in their application? “

The answers to these questions should be given by an effective security program. As noted by NIST [14];

“An effective information security program should include:

- **Periodic assessments of risk**, including the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the organization

- **Policies and procedures** that are based on risk assessments, cost-effectively reduce information security risks to an acceptable level and address information security throughout the life cycle of each organizational information system
- **Plans for providing adequate information security** for networks, facilities, information systems, or groups of information systems, as appropriate;
- **Security awareness training** to inform personnel (including contractors and other users of information systems that support the operations and assets of the organization) of the information security risks associated with their activities and their responsibilities in complying with organizational policies and procedures designed to reduce these risks;
- **Periodic testing and evaluation of the effectiveness of information security policies**, procedures, practices, and security controls to be performed with a frequency depending on risk, but no less than annually;
- **A process for planning, implementing, evaluating, and documenting remedial actions** to address any deficiencies in the information security policies, procedures, and practices of the organization;
- **Procedures for detecting, reporting, and responding to security incidents**
- **Plans and procedures for continuity of operations** for information systems that support the operations and assets of the organization

It is of paramount importance that responsible officials within the organization understand the risks and other factors that could adversely affect organizational operations, organizational assets, or individuals. Moreover, these officials must understand the current status of their security programs and the security controls planned or in place to protect their information systems in order to make informed judgments and investments that appropriately mitigate risks to an acceptable level."

4.2 Security Control Baselines

The challenge for organizations is to determine the appropriate set of security controls, which if implemented and determined to be effective in their application, would most cost-effectively comply with the stated security requirements. Selecting the appropriate set of security controls to meet the specific, and sometimes unique, security requirements of an organization is an important task—a task that demonstrates the organization's commitment to security and the due diligence exercised in protecting the confidentiality, integrity, and availability of their information and information systems.

In order assist organizations in making the appropriate selection of security controls for their information systems, the concept of baseline controls is introduced. Baseline controls are the minimum security controls recommended for an information system based on the system's security categorization in accordance with FIPS 199[3] standard NIST [15]. The tailored security control baseline serves as the starting point for organizations in determining the appropriate safeguards and countermeasures necessary to protect their information systems. Because the baselines are intended to be broadly applicable starting points, supplements to the tailored baselines will likely be necessary in order to achieve adequate risk mitigation. The tailored baselines are supplemented based on organizational assessments of risk and the resulting controls documented in the security plans for the information systems.

Section 4.5 provides a listing of baseline security controls. Three sets of baseline controls have been identified corresponding to the low-impact, moderate-impact, and high-impact levels. Each of the three baselines provides an initial set of security controls for a particular impact level associated with a security category given by NIST [15].

[3] FIPS 199; is a Standard for security categorization of federal information systems in United States of America.

4.3 Common Security Controls

An organization-wide view of an information security program facilitates the identification of common security controls that can be applied to one or more organizational information systems. As noted by NIST [14];

“Common security controls can apply to:

- all organizational information systems;
- a group of information systems at a specific site; or
- Common information systems, subsystems, or applications (i.e., common hardware, software, and/or firmware) deployed at multiple operational sites. Common security controls have the following properties:

The development, implementation, and assessment of common security controls can be assigned to responsible organizational officials or organizational elements (other than the information system owners whose systems will implement or use the common security controls); and the results from the assessment of the common security controls can be used to support the security certification and accreditation processes of organizational information systems where the controls have been applied.”

The identification of common security controls is most effectively accomplished as an organization-wide exercise with the involvement of the chief information officer, senior agency information security officer, authorizing officials, information system owners/program managers, information owners, and information system security officers.

Many of the security controls needed to protect an information system (e.g., contingency planning controls, incident response controls, security training and awareness controls, personnel security controls, physical and environmental protection controls, and intrusion detection controls) may be excellent candidates for common security control status. By centrally managing the development, implementation, and assessment of the common security controls designated by the organization, security costs can be amortized across multiple information systems. Security controls not designated as common controls are considered system-specific controls and are the responsibility of the information system owner. Security plans for individual information systems should clearly identify which security controls have been designated by the organization as common security controls and which controls have been designated as system-specific controls.

Organizations may also assign a hybrid status to security controls in situations where one part of the control is deemed to be common, while another part of the control is deemed to be system-specific. For example, an organization may view the Incident Response Policy and Procedures security control as a hybrid control with the policy portion of the control deemed to be common and the procedures portion of the control deemed to be system-specific. Hybrid controls may also serve as templates for further control refinement. An organization may choose, for example, to implement the Contingency Planning security control as a master template for a generalized contingency plan for all organizational information systems with individual information system owners tailoring the plan, where appropriate, for system-specific issues.

Information system owners are responsible for any system-specific issues associated with the implementation of an organization's common security controls. These issues are identified and described in the system security plans for the individual information systems. The senior agency information security officer, acting on behalf of the chief information officer, should coordinate with organizational officials (e.g., facilities managers, site managers, personnel managers) responsible for the development and implementation of the designated common security controls to ensure that the required controls are put into place, the controls are assessed, and the assessment results are shared with the appropriate information system owners to better support the security accreditation process.

Partitioning security controls into common controls and system-specific controls can result in significant savings to the organization in development and implementation costs especially when the common controls serve multiple information systems and entities. It can also result in a more consistent application of the security controls across the organization at large. Moreover, equally significant savings can be realized in the security certification and accreditation process. Rather than assessing common security controls in every information system, the certification process draws upon any applicable results from the most current assessment of the common security controls performed at the organization level. An organization-wide approach to reuse and sharing of assessment results can greatly enhance the efficiency of the security certifications and accreditations being conducted by organizations and significantly reduce security program costs.

While the concept of security control partitioning into common security controls and system-specific controls is straightforward and intuitive, the application of this principle within an organization takes planning, coordination, and perseverance. If an organization is just beginning to implement this approach or has only partially implemented this approach, it may take some time to get the maximum benefits from security control partitioning and the associated reuse of assessment evidence. Because of the potential dependence on common security controls by many of an organization's information systems, a failure of such common controls may result in a significant increase in agency-level risk—risk that arises from the operation of the systems that depend on these controls.

4.4 Security Categorization

The security controls applied to a particular information system should be proportionate with the potential impact on organizational operations, organizational assets, or individuals should there be a loss of confidentiality, integrity, or availability. FIPS 199 requires organizations to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability. The potential impact values assigned to the respective security objectives are the highest values from among the security categories that have been determined for each type of information resident on those information systems. The generalized format for expressing the security category (SC) of an information system is:

$$\boldsymbol{SC_{IS}} = \{(\boldsymbol{Confidentiality}, impact), (\boldsymbol{Integrity}, impact), (\boldsymbol{Availability}, impact)\} \qquad (4.1)$$

Since the potential impact values for confidentiality, integrity, and availability may not always be the same for a particular information system, the high water mark concept is used to determine the impact level of the information system for the express purpose of selecting an initial set of security controls from one of the three security control baselines. High water mark method used in this issue determines the security categorization of an IS by selecting the highest level regardless of the other two lower levels. Thus, a low-impact system is defined as an information system in which all three of the security objectives are low. A moderate-impact system is an information system in which at least one of the security objectives is moderate and no security objective is greater than moderate. And finally, a high-impact system is an information system in which at least one security objective is high.

4.5 Selected Security Controls

According to the security categorization NIST[4] recommends baseline security controls for each impact level. A list of selected technical security controls are given below in Tables 4.1,4.2, 4.3 and 4.4. In the application chapter, these controls will be mapped to related security products to employ security controls that are appropriate to the categorization of the chosen organization.

[4] NIST; National Institute of Standards and Technology, is a measurement standards laboratory which is a non-regulatory agency of the United States Department of Commerce.

Table 4.1 Selected security controls in access control family.

Access Control Family	Low	Moderate	High
Access Control Policy and Procedures	Selected	Selected	Selected
Account Management	Selected	Selected	Selected
Access Enforcement	Selected	Selected	Selected
Information Flow Enforcement	---	Selected	Selected
Separation of Duties	---	Selected	Selected
Least Privilege	---	Selected	Selected
Unsuccessful Login Attempts	Selected	Selected	Selected
System Use Notification	Selected	Selected	Selected
Previous Logon Notification	---	---	---
Concurrent Session Control	---	---	Selected
Session Lock	---	Selected	Selected
Session Termination	---	Selected	Selected
Supervision and Review—Access Control	Selected	Selected	Selected
Permitted Actions without Identification or Authentication	Selected	Selected	Selected
Automated Marking	---	---	Selected
Automated Labeling	---	---	---
Remote Access	Selected	Selected	Selected
Wireless Access Restrictions	Selected	Selected	Selected
Access Control for Portable and Mobile Devices	---	Selected	Selected
Use of External Information Systems	Selected	Selected	Selected

Table 4.2 Selected security controls in audit and accountability family.

Audit And Accountability	Low	Moderate	High
Audit and Accountability Policy and Procedures	Selected	Selected	Selected
Auditable Events	Selected	Selected	Selected
Content of Audit Records	Selected	Selected	Selected
Audit Storage Capacity	Selected	Selected	Selected
Response to Audit Processing Failures	Selected	Selected	Selected
Audit Monitoring, Analysis, and Reporting	---	Selected	Selected
Audit Reduction and Report Generation	---	Selected	Selected
Time Stamps	Selected	Selected	Selected
Protection of Audit Information	Selected	Selected	Selected
Non-repudiation	---	---	---
Audit Record Retention	Selected	Selected	Selected

Table 4.3 Selected security controls in identification and authentication family.

Identification and Authentication	Low	Moderate	High
Identification and Authentication Policy and Procedures	Selected	Selected	Selected
User Identification and Authentication	Selected	Selected	Selected
Device Identification and Authentication	---	Selected	Selected
Identifier Management	Selected	Selected	Selected
Authenticator Management	Selected	Selected	Selected
Authenticator Feedback	Selected	Selected	Selected
Cryptographic Module Authentication	Selected	Selected	Selected

Table 4.4 Selected security controls in system and communication protection family.

Systems and Communication Protection	Low	Moderate	High
System and Communications Protection Policy and Procedures	Selected	Selected	Selected
Application Partitioning	---	Selected	Selected
Security Function Isolation	---	---	Selected
Information Remnance	---	Selected	Selected
Denial of Service Protection	Selected	Selected	Selected
Resource Priority	---	---	---
Boundary Protection	Selected	Selected	Selected
Transmission Integrity	---	Selected	Selected
Transmission Confidentiality	---	Selected	Selected
Network Disconnect	---	Selected	Selected
Trusted Path	---	---	---
Cryptographic Key Establishment	---	Selected	Selected
Use of Cryptography	Selected	Selected	Selected
Public Access Protections	Selected	Selected	Selected
Collaborative Computing	---	Selected	Selected
Transmission of Security Parameters	---	---	---
Public Key Infrastructure Certificates	---	Selected	Selected
Mobile Code	---	Selected	Selected
Voice Over Internet Protocol	---	Selected	Selected
Secure Name /Address Resolution Service	---	Selected	Selected
Architecture and Provisioning for Name/Address Resolution Service	---	Selected	Selected
Session Authenticity	---	Selected	Selected

5. INFRASTRUCTRAL SECURITY PRODUCTS

Organization and most of the content of this chapter is borrowed from a publication of NIST [16].

5.1 Identification and Authentication

Identification is the means by which a user provides a claimed identity to the system. Authentication is the means of establishing the validity of this claim. Authorization is the process of defining and maintaining the allowed actions. Identification and authentication establishes the basis for accountability and the combination of all three enables the enforcement of identity-based access control. The user's identity can be authenticated using the following mechanisms:

- Requiring the user to provide something they have (e.g., **token**)
- Requiring the user to provide something they alone know (e.g., **password**)
- Sampling a personal characteristic (e.g., **fingerprint**).

The principal forms of authentication include static, dynamic, and multiple factor:

- **Static authentication** reuses a specific authenticator (e.g., static password). This type of authentication only provides protection against attacks in which an imposter cannot obtain the authenticator. The strength of the authentication process is highly dependent on the difficulty of guessing or decrypting the authenticator values and therefore how well they are protected in transit and while stored on the system.
- **Dynamic authentication** uses cryptography or other techniques to create one per-session authenticator. A dynamic authenticator changes with each authentication session between the claimant and verifier.
- **Multiple-factor authentication** requires two or more types of authentication techniques. Multiple factor authentication can include both static and dynamic authentication mechanisms. One example is the use of a password along with a smart card token.

Authorization mechanisms fall into four major categories:

- **Local:** Local authorization is performed for each application and machine to which a user requires access. The mechanisms of the local operating system and applications are employed to setup and maintain the authorizations for that machine or application.
- **Network**: Authorization is performed at a central, authorization server, providing access to a user's account from one or more workstations on the network. The key here is that the access is to a single user account. If the user requires multiple accounts, then each is a separate authorization and handled in like manner to multiple users.
- **Single Sign-on**: Single sign-on employs a central authorization server to enable a user to authenticate one time in order to achieve access to multiple applications, machines, and domains operating with a variety of authentication mechanisms (for example, a Kerberos[5] implementation within a heterogeneous Windows 2000 and Unix network). The central server contains identifier/authenticator pairs for each domain that the user needs to access and performs an authentication on behalf of the user for each resource that the user is authorized to access. The central server establishes and maintains, as individual actions, the authorizations at each application, machine, or domain that the user is allowed to access.
- **Single Log-on**: Single log-on is similar to single sign-on with the exception that the central server authentication mechanism is the mechanism used by all the applications, machine, and domains with which the user needs to interact. Rather than store identifier/authenticator pairs for each verification, the one-time verification is accepted by all resources as the only verification needed. Additionally, the authorizations are maintained at the central server and the individual applications, machines, and domains query the central location to determine whether a specific access is authorized.

[5] Kerberos; is a secure network authentication method for a service in a computer network.

Some examples of authentication products are provided below. These categories of authentication products are not mutually exclusive (e.g., some products may include one or more of the categories).

Security Tokens: Security tokens are used to allow access first to a computer and then to a network. Tokens come in various forms - for example, Personal Computer Memory Card International Association (PCMCIA) cards, flash memory, USB tokens, smart cards, and software.

- PCMCIA Security Tokens: These tokens offer a full suite of security services in portable format on a small card. PCMCIA cards can protect secret values adequately in most cases while still leaving room for additional physical tamper protection mechanisms. Disadvantages include a requirement for a PCMCIA card reader. Although common on laptop computers, PCMCIA card readers are not common in desktop computers. This imposes a significant added cost factor. The added expense of purchasing a card reader for every desktop workstation may be cost prohibitive especially in organizations with large numbers of desktop computers.
- Smart Card Tokens: Smart cards are replacing PCMCIA cards in many security token applications. Smart cards are credit-card size plastic cards with an embedded computer chip. The chip can be either a microprocessor with internal memory or a memory chip with nonprogrammable logic. The chip connection is made by either direct physical contact or remotely via a contactless electromagnetic interface.

Certificates: The public key certificate associates a certificate holder's identity with his public key. (See Section 5.5, Public Key Infrastructure, for further details)

Authentication Protocols: These protocols are used to determine who is accessing a resource.

An example can be Radius:

- RADIUS: Using the Remote Authentication Dial-In User Service (RADIUS) protocol, a remote client can exchange authentication, access control, accounting, and device configuration information with a RADIUS server. The RADIUS server can authenticate a user or a device from its database or user I&A parameters.

Biometrics: Biometrics are used for physical access control, electronic access control, and monitoring devices. An organization’s choice of biometric control depends on the security level required, user acceptance, enrollment speed, and costs incurred. Biometrics technology is used to identify and authenticate an individual based on personal characteristics. Examples of personal characteristics include fingerprints, face, retina, iris, speech, handwriting, hand geometry, and wrist veins. Biometrics can also be combined with passwords, personal identification numbers (PIN), and cards to further increase accuracy and security.

5.2 Access Control

Access control ensures that only authorized access to resources occurs. Access control helps protect confidentiality, integrity, and availability and supports the principles of legitimate use, least privilege, and separation of duties. Access control simplifies the task of maintaining enterprise network security by reducing the number of paths that attackers might use to penetrate system or network defenses.

Access control systems grant access to information system resources to authorized users, programs, processes, or other systems. Access control may be managed solely by the application, or it may use controls on files. The system may put classes of information into files with different access privileges. Controlling access can be based on any or a combination of the following:

- User identity
- Role memberships
- Group membership
- Other information known to the system.

By controlling who can use an application, database record, or file, an organization can help to protect that data. It is particularly important to control who is allowed to enable or disable the security features or to change user privileges.

Users need to ensure that secure applications sufficiently manage access to data that they maintain. Access control includes any or all of the following: knowing who is attempting access, mediating access according to some processing rules, and managing where or how data is sent.

Access Control Lists: Access control data can reside either in (a) the resource to be protected or (b) a central location based on a model. An example of a data structure used for resource-centric storage of access control information is the Access Control List (ACL). An example of a specification of access control information centrally based on a model is the role-based access control (RBAC) database.

ACLs in routers and other network devices can be used to implement the following forms of access enforcement:

Traffic Filters: Access controls can be enforced effectively at the data packet layer. A filter can block any packet that does not conform to security policy rules. Filters can be assigned to incoming or outgoing traffic. Filtering can be based on source and destination addresses, protocol types, and information from other fields within the packets unless the content is encrypted.

Policy Filters: Policy filters can be used to set up access control policies on routers. Policy filters, which operate to and from routing tables, can be used to specify the routers or networks from which updates will be accepted.

Role-Based Access Control: (RBAC) has emerged as a promising feature of many database management, security management and network operating system products. The essential advantage of RBAC products is that they allow system administrators to assign individual users into roles. The role identifies users as members of a specific group, based on their capabilities, work requirements, and responsibilities in the organization. Access rights, or security privileges, are then established for each role; a user may belong to multiple roles, which provide the appropriate level of access for their requirements. Thus, the RBAC structure empowers administrators with a tool to regulate which users are given access to certain data or resources, without having to explicitly authorize each user to each resource.

5.3 Intrusion Detection and Prevention

Intrusion detection is the process of monitoring events occurring in a computer system or network and analyzing them for signs of intrusions, defined as attempts to perform unauthorized actions, or to bypass the security mechanisms of a computer or network. Intrusions are caused by any of the following: attackers who access systems from the Internet, authorized system users who attempt to gain additional privileges for which they are not authorized and authorized users who misuse the privileges given them. Intrusion detection systems (IDS) are software or hardware products that assist in the intrusion monitoring and analysis process.

The implementation of IDS might be valuable for the following reasons:

- Prevent problem behaviors by increasing risk of discovery and punishment for system intruders
- Detect attacks and other security violations that are not prevented by other security measures
- Detect preambles to attacks (network probes and other tests for existing vulnerabilities)
- Document the existing threat to the organization
- Quality control for security design and administration
- Provide useful information about methods used in intrusions.

There are two different approaches to analyzing events to detect attacks: signature-based detection and anomaly detection. Either or both of the approaches could be used in an IDS product.

- **Signature-Based Detection:** This approach identifies events or sets of events that match with a predefined pattern of events that describe a known attack. These patterns are called signatures. Signatures may include system states, or accessing system areas that have been explicitly identified as “off-limits.”

- **Anomaly Detection:.** Anomaly detection assumes that all intrusive activities deviate from the norm. These tools typically establish a normal activity profile and then maintain a current activity profile of a system. When the two profiles vary by statistically significant amounts, an intrusion attempt is assumed

Three common types of IDS products are network based, host based, and application based. Each type of product may optionally offer intrusion prevention capabilities.

Network-Based IDS: 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. 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. Because 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”[6], making it more difficult for an attacker to determine their presence and location.

Host-Based IDS: Host-based IDSs operate on information collected from within an individual computer system. This vantage point allows host-based IDSs to determine exactly which processes and user accounts are involved in a particular attack on the OS. Furthermore, unlike network-based IDSs, host-based IDSs can more readily “see” the intended outcome of an attempted attack, because they can directly access and monitor the data files and system processes usually targeted by attacks. Host-based IDSs normally use information sources of two types: operating system audit trails, and system logs. Operating system audit trails are

[6] Stealth Mode; in Network IPS and IDS systems refer to a completely passive device which its presence is difficult to certainly detect.

usually generated at the innermost (kernel) level of the operating system; therefore these trails are more detailed and better protected than system logs. 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.

Application-Based IDS: 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 attempting to exceed their authorization. This is because such problems are more likely to appear in the interaction among the user, the data, and the application.

Intrusion Prevention: Intrusion detection systems often have intrusion prevention capabilities. This means that not only can they detect an intrusive activity, but they can also attempt to stop the activity, ideally before it reaches its targets. Intrusion prevention is much more valuable than intrusion detection because intrusion detection simply observes events without making any effort to stop them. Unfortunately, intrusion prevention can also cause operational issues because if the detection of incidents is not accurate, then it may block legitimate activities that are incorrectly classified as malicious. Any organization that wants to utilize intrusion prevention should pay particular attention to detection accuracy when selecting a product.

Another consideration involving intrusion prevention is architecture-related. IDS products may be simply monitoring activity, or they may actually be “in-line”, which means that activity must pass through them. Examples include a network-based IDS that is integrated with a firewall and a host-based IDS that is integrated into the kernel of the operating system. An in-line intrusion detection system has the ability to block all detected attacks. If an IDS product is not in-line, its ability to block attacks may be limited.

5.4 Firewall

Firewalls are devices or systems that control the flow of network traffic between networks or between a host and a network. A firewall acts as a protective barrier because it is the single point through which communications pass. Internal information that is being sent can be forced to pass through a firewall as it leaves a network or host. Incoming data can enter only through the firewall.

While firewalls and firewall environments are often discussed in the context of Internet connectivity, firewalls have applicability in network environments beyond Internet connectivity. For example, many corporate enterprise intranets employ firewalls to restrict connectivity to and from internal networks servicing more sensitive functions, such as the accounting or personnel department. By employing firewalls to control connectivity to these areas, an organization can prevent unauthorized access to the respective systems and resources within the more sensitive areas. The inclusion of an internal firewall environment can therefore provide an additional layer of security that would not otherwise be available.

Although firewalls afford protection of certain resources within an organization, there are some threats that firewalls cannot protect against: connections that bypass the firewall, new threats that have not yet been identified, and viruses that have been injected into the internal network. It is important to remember these shortcomings because considerations will have to be made in addition to the firewall in order to counter these additional threats and provide a more comprehensive security solution.

There are nine type of firewalls. Their short definitions are given below.

1. **Packet Filter Firewalls**: The most basic firewall is called a packet filter. Packet filter firewalls are routing devices that include access control functionality for system addresses and communication sessions. The

access control functionality of a packet filter firewall is governed by a set of directives collectively referred to as a rule set.

Packet filter firewalls have two main strengths: speed and flexibility. Packet filter firewalls can be used to secure nearly any type of network communication or protocol. This simplicity allows packet filter firewalls to be deployed into nearly any enterprise network infrastructure. Note that their speed, flexibility, and capability to block denial-of-service and related attacks make them ideal for placement at the outermost boundary with an untrusted network.

Packet filter firewalls possess several weaknesses:

- Because packet filter firewalls do not examine upper-layer data, they cannot prevent attacks that employ application-specific vulnerabilities or functions.
- Because of the limited information available to the firewall, the logging functionality present in packet filter firewalls is limited. Packet filter logs normally contain the same information used to make access control decisions (source address, destination address, and traffic type).
- A firewall relying solely on packet filtering would not support advanced user authentication schemes.

They are vulnerable to attacks and exploits that take advantage of flaws within the TCP/IP specification and protocol stack, such as network layer address spoofing[7].

Consequently, packet filter firewalls are very suitable for high-speed environments where logging and user authentication with network resources are not important.

[7] Address spoofing; in networking is the act of forging network packets with false source addresses to conceal the identity of the sender.

An example of a packet-filter firewall is a network router employing filter rules to screen network traffic.

2. **Stateful Inspection Firewalls:** Stateful inspection evolved from the need to accommodate certain features of the TCP/IP[8] protocol suite. When an application uses a TCP (connection-oriented transport) to create a session with a remote host system, a port is also created on the source system. This port receives network traffic from the destination system. Packet filter firewalls must permit inbound network traffic on all return packets from the destination system for connection-oriented transport to occur. Opening this many ports creates an immense risk of intrusion by unauthorized users who may employ a variety of techniques to abuse the expected conventions. Stateful inspection firewalls solve this problem by creating a directory of outbound TCP connections, along with each session's corresponding client port. This "state table" is then used to validate any inbound traffic. The stateful inspection solution is more secure because the firewall tracks client ports individually rather than opening all inbound ports for external access.

   Stateful inspection firewalls share the strengths and weaknesses of packet filter firewalls, but because of the state table implementation, stateful inspection firewalls are generally considered to be more secure than packet filter firewalls.

   Stateful inspection firewalls can accommodate other network protocols in the same manner as packet filters, but the actual stateful inspection technology is relevant only to TCP/IP. For this reason, many texts classify stateful inspection firewalls as representing a superset of packet filter firewall functionality.

3. **Application-Proxy Gateway Firewalls:** Application proxy gateway firewalls provide additional protection by inserting the application in the communications path, looking like the end-point of the communications to

[8] TCP/IP; is a communication protocol which internet or similar networks use to communicate.

both sides of the firewall. For example, a web-proxy receives requests for external, web access from inside the firewall and relays them to the exterior web page as though the firewall was the requesting web client. The external web page responds to the firewall and the firewall forwards the response to the inside client as though the firewall was the web server. No through TCP/IP connection is ever made from inside client to external web server.

Application-proxy gateway firewalls have numerous advantages over packet filter firewalls and stateful inspection packet filter firewalls. First, application-proxy gateway firewalls usually have more extensive logging capabilities resulting from the firewall being able to examine the entire network packet rather than only the network addresses and ports.

Another advantage is that application-proxy gateway firewalls allow security administrators to enforce whatever type of user authentication is considered appropriate for a given enterprise infrastructure. Application-proxy gateways can authenticate users directly, as opposed to packet filter firewalls and stateful inspection packet filter firewalls, which normally authenticate users based on the network layer address of the system on which they reside (i.e., source, destination, and type). Given that network layer addresses can be easily spoofed, the authentication capabilities inherent in application-proxy gateway architecture are superior to those found in packet filter or stateful inspection packet filter firewalls.

The advanced functionality of application-proxy gateway firewalls also fosters several disadvantages when compared with packet filter or stateful inspection packet filter firewalls. First, because of the “full packet awareness” found in application-proxy gateways, the firewall is forced to spend significant time reading and interpreting each packet. Therefore, application-proxy gateway firewalls are not generally well suited to high-bandwidth or real-time applications. To reduce the load on the firewall, a dedicated proxy server can be used to secure less time-sensitive services, such as e-mail and most Web traffic. Another disadvantage is that application-proxy gateway firewalls are often limited in terms of support for new network applications and protocols. An individual, application-specific proxy agent is required for each type of network traffic that needs to transit a firewall. Most application-proxy gateway firewall vendors provide generic proxy agents to support undefined network protocols or applications. However, those generic agents tend to negate many of the strengths of the application-proxy gateway architecture, and they simply allow traffic to “tunnel” through the firewall.

4. **Dedicated Proxy Firewalls:** Dedicated proxy servers differ from application-proxy gateway firewalls in that they retain proxy control of traffic, but they do not contain firewall capability. They are typically deployed behind traditional firewall platforms for this reason. In typical use, a main firewall might accept inbound traffic, determine which application is being targeted, and then hand off the traffic to the appropriate proxy server (e.g., an e-mail proxy server). The proxy server typically would perform filtering or logging operations on the traffic and then forward it to internal systems. A proxy server could also accept outbound traffic directly from internal systems, filter or log the traffic, and then pass it to the firewall for outbound delivery.

   Dedicated proxies allow an organization to enforce user authentication requirements and other filtering and logging on any traffic that traverses the proxy server. The implications are that an organization can restrict outbound traffic to certain locations or could examine all outbound e-mail for viruses or restrict internal users from writing to the organization’s Web server. Security experts have stated that most security problems occur from within an organization; proxy servers can assist in foiling internally based attacks or malicious behavior. Simultaneously, filtering outbound traffic will place a heavier load on the firewall and increase administration costs. Many organizations enable the caching of frequently used Web pages on the proxy, thereby reducing firewall traffic. In addition to authentication and logging functionality, dedicated proxy servers are useful for Web and electronic mail (e-mail) content scanning.

5. **Hybrid Firewall Technologies:** Recent advances in network engineering and IS security have resulted in a “blurring of the lines” that differentiates

the various firewall platforms discussed earlier. As a result, firewall products currently incorporate functionality from several different classifications of firewall platforms. For example, many packet filter or stateful inspection packet filter firewall vendors have implemented basic application-proxy functionality to offset some of the weaknesses associated with their firewall platform. In most cases, packet filter or stateful inspection packet filter firewall vendors implement application proxies to provide improved network traffic logging and user authentication in their firewalls. Nearly all major firewall vendors have introduced hybridization into their products in some manner; therefore it is not always a simple matter to decide which specific firewall product is the most suitable for a given application or enterprise infrastructure. Hybridization of firewall platforms makes the prepurchase product evaluation phase of a firewall project important. Supported feature sets, rather than firewall product classification, should drive the product selection.

6. **Network Address Translation**: Network address translation (NAT) technology was developed in response to two major issues in network engineering and security. Network address translation is an effective tool for "hiding" the network-addressing schema present behind a firewall environment. In essence, NAT allows an organization to deploy an addressing schema of its choosing behind a firewall, while still maintaining an ability to connect to external resources through the firewall. Network address translation is accomplished by one of three methods: static, hiding, and port.

   In static NAT, each internal system on the private network has a corresponding external, routable IP address associated with it. This particular technique is seldom used because of the scarcity of available IP address resources.

   With hiding NAT, all systems behind a firewall share the same external, routable IP address. Thus, with a hiding NAT system, many systems behind a firewall will still appear as only one system. With port address translation, it is possible to place resources behind a firewall system and still make them selectively accessible to external users.

In terms of strengths and weaknesses, each type of NAT has applicability in certain situations, with the variable being the amount of design flexibility offered by each type. Static NAT offers the most flexibility, but as stated earlier, static NAT is not always practical given the shortage of IP version 4 addresses. Hiding NAT technology was an interim step in the development of NAT technology, but it is seldom used because port address translation offers additional features beyond those present in hiding NAT while maintaining the same basic design and engineering considerations. Port address translation is often the most convenient and secure solution.

7. **Host-based Firewalls:** Firewall packages are available in some OSs or as add-ons; they can be used to secure only the individual host. Internal servers should be protected and should not be assumed to be safe from attack because they are behind a main firewall. Host-based firewall packages typically provide access-control capability for restricting traffic to and from servers running on the host, and logging is usually available. A disadvantage to host-based firewalls is that they must be administered separately and maintaining security becomes more difficult as the number of devices to be configured increases. A sample topology for host-based firewall is given in the Figure 5.1.

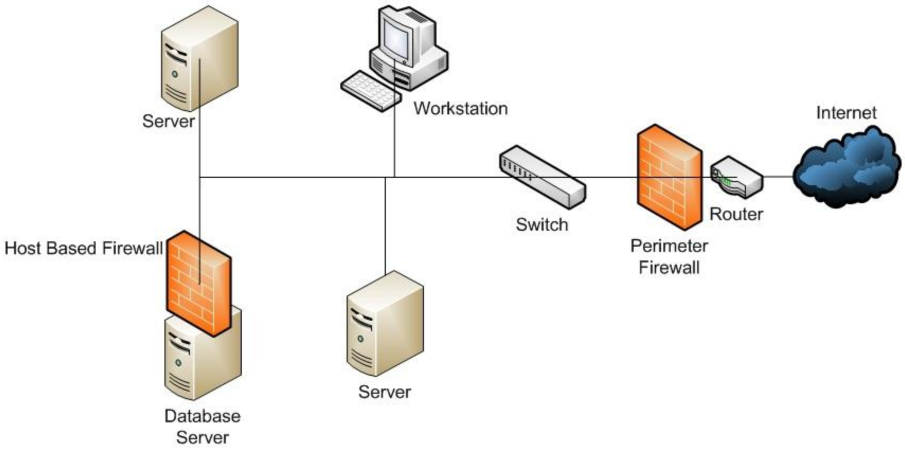


Figure 5.1 Host-based firewall

In this topology internet traffic is passing through router[9], perimeter firewall and internal switch[10] respectively. There is no available security device, besides the host-based firewall in place, to limit the access of the workstation on the database server.

8. **Personal Firewalls/Personal Firewall Appliances:** Securing personal computers (PC) at home or remote locations is now as important as securing them at the office; many personnel telecommute or work at home and operate on organization- or agency-proprietary data. Home users dialing an Internet service provider (ISP) may have limited firewall protections available to them because the ISP has to accommodate potentially many different security policies. Therefore, personal firewalls have been developed to provide protection for remote systems and to perform many of the same functions as larger firewalls. These products are typically implemented in one of two configurations.

   The first configuration is a personal firewall, which is installed on the system it is meant to protect; personal firewalls usually do not offer protection to other systems or resources. Likewise, personal firewalls do not typically provide controls over network traffic that is traversing a computer network — they protect only the computer system on which they are installed.

   The second configuration is a personal firewall appliance, which is in concept similar to a traditional firewall. In most cases, personal firewall appliances are designed to protect small networks such as networks that might be found in home offices. These appliances usually run on specialized hardware and integrate some other form of network infrastructure components in addition to the firewall itself, including the following: broadband modem wide area network (WAN) routing, LAN

[9] Router; is a network devices that is connected to more than one network to handle the traffic between them.

[10] Switch; is a network device to connect computers in order to establish a network.

routing (dynamic routing support), network hub, network switch, Dynamic Host Configuration Protocol (DHCP) server, Simple Network Management Protocol (SNMP) agent, and application-proxy agents.

In terms of deployment strategies, personal firewalls and personal firewall appliances normally address connectivity concerns associated with telecommuters or branch offices. However, some organizations employ these devices on the organizational intranet, practicing a layered defense strategy.

Management of the device or application is an important factor when evaluating or choosing a personal firewall or personal firewall appliance. Ideally, a personal firewall or personal firewall appliance should enable the organization or agency to enforce its defined security posture on all systems that connect to its networks and systems. In the case of telecommuters, this means that a personal firewall or personal firewall appliance should enforce a policy at least as restrictive as end-users would experience if they were behind the corporate or agency firewall in the office.

9. **Centrally Managed Distributed Firewalls:** The goals for host-based firewalls and personal firewalls/appliances can also be achieved using centrally managed distributed firewall products. All of these firewall types provide firewall capability in every protected computer. Centrally managed distributed firewalls are centrally controlled but locally enforced. A security administrator defines and maintains security policies, not the end-users. This places the responsibility and capability of defining security policies in the hands of a security professional who can properly lock down the target systems. A centrally managed system is scalable because each system does not have to be administered separately. A properly executed distributed firewall system includes exception logging. More advanced systems include location intelligence so that the appropriate policy is enforced depending on the context of the connection.

   Centrally managed distributed firewalls can be either software- or hardware-based firewalls. Centrally managed distributed software firewalls are similar in function and features to host-based or personal firewalls, but the security policies are centrally defined and managed. Software distributed firewalls have the benefit of unified corporate oversight of firewall implementation on individual machines, however they remain vulnerable to attacks on the host operating system from the networks, as well as intentional or unintentional tampering by users logging into the system being protected. Centrally managed distributed hardware firewalls combine the filtering capability of a firewall with the connectivity capability of a traditional connection. Filtering the data on the firewall hardware rather than the host system can make this system less vulnerable than software-based distributed firewalls. Hardware distributed firewalls can be designed to be unaffected by local or network attacks via the host operating systems. Performance and throughput of a hardware system is generally higher than software systems

5.5 Malicious Code Protection

Viruses, worms and other malicious codes are typically hidden in software and require a host to replicate. Malicious code protection requires strict procedures and multiple layers of defense. Protection includes prevention, detection, containment, and recovery. Protection hardware and access-control software can inhibit this code as it attempts to spread. Most security products for detecting malicious code include several programs that use different techniques such as scanners, integrity checkers, vulnerability monitors and behavioral blockers.

Scanners: Scanners provide precise identification of known malicious code. Scanners search for “signature strings” or use algorithmic detection methods to identify known code. Scanners rely on a significant amount of a prior knowledge about the code. Therefore, it is critical that the signature information for scanners is current. Most scanners can be configured to automatically update their signatures from a designated source, typically on a weekly basis; scanners can also be forced to update their signatures on demand.

Integrity Checkers: Integrity checkers detect infections by searching a program or other executable code to determine if it has been altered or changed. Integrity checkers can only flag a change as suspicious; they cannot determine if the change is a genuine virus infection. These programs are usually checksum based. The integrity checking process begins with the creation of a baseline, where checksums for clean executables are computed and saved. Each time the integrity checker is run, it again makes a checksum computation and compares the result with the stored value. Note that several different kinds of checksums are used. Simple checksums are easy to defeat; cyclical redundancy checks (CRC) are better, but can still be defeated. Cryptographic checksums such as SHA provide the highest level of security.

Vulnerability Monitors: These monitors are designed to prevent modification or access to particularly sensitive parts of the system; consequently, the monitors may block an attack on those parts. This requires considerable information about “normal” system use because PC viruses typically take advantage of system vulnerabilities and do not circumvent any security features. This type of software also requires decisions from the user about permitted operations.

Behavior Blockers: These programs contain a list of rules that a legitimate program must follow. If the program breaks one of the rules, the behavior blockers alert the users. The “sandbox” concept is that untrusted code is first checked for improper behavior. If none is found, it can be run in a restricted environment, where dynamic checks are performed on each potentially dangerous action before it is permitted to take effect. By adding multiple layers of reviews and checks to the execution process, behavior blockers can prevent malicious code from performing undesirable actions.

5.6 Physical Security

In this section, the types of physical situations and occurrences that can constitute a threat to information systems is given. There are a number of ways in which such threats can be categorized. It is important to understand the spectrum of threats to information systems so that responsible administrators can ensure that prevention measures are comprehensive.

Threats can be organized into the following categories:

- Environmental threats
- Technical threats
- Human-caused Physical threats

First natural disasters are discussed, which are a prime, but not the only, source of environmental threats. Then environmental threats followed by technical and human-caused threats given by Vacca [2].

5.6.1 Environmental threats

Natural disasters are the source of a wide range of environmental threats to datacenters, other information processing facilities, and their personnel. It is possible to assess the risk of various types of natural disasters and take suitable precautions so that catastrophic loss from natural disaster is prevented. Table 5.1 given by Vacca[2] lists six categories of natural disasters, the typical warning time for each event, whether or not personnel evacuation is indicated or possible, and the typical duration of each event.

A tornado can generate winds that exceed hurricane strength in a narrow band along the tornado’s path. There is substantial potential for structural damage, roof damage, and loss of outside equipment. There may be damage from wind and flying debris. Off site, a tornado may cause a temporary loss of local utility and communications. Offsite damage is typically followed by quick restoration of services.

A hurricane, depending on its strength, may also cause significant structural damage and damage to outside equipment. Off site, there is the potential for severe region wide damage to public infrastructure, utilities, and communications. If onsite operation must continue, then emergency supplies for personnel as well as a backup generator are needed. Further, the responsible site manager may need to mobilize private post-storm security measures, such as armed guards.

Table 5.1 Characteristics of natural disasters

	Warning	Evacuation	Duration
Tornado	Advance warning of potential; not site specific	Remain at site	Brief but intense
Hurricane	Significant advance warning	May require evacuation	Hours to a few days
Earthquake	No warning	May be unable to evacuate	Brief duration; threat of continued aftershocks
Ice storm/blizzard	Several days warning generally expected	May be unable to evacuate	May last several days
Lightning	Sensors may provide minutes of warning	May require evacuation	Brief but may recur
Flood	Several days warning generally expected	May be unable to evacuate	Site may be isolated for extended period

A major earthquake has the potential for the greatest damage and occurs without warning. A facility near the epicenter may suffer catastrophic, even complete, destruction; with significant and long-lasting damage to datacenters and other IS facilities. Examples of inside damage include the toppling of unbraced computer hardware and site infrastructure equipment, including the collapse of raised floors. Personnel are at risk from broken glass and other flying debris. Off site, near the epicenter of a major earthquake, the damage equals and often exceeds that of a major hurricane. Structures that can withstand a hurricane, such as roads and bridges, may be damaged or destroyed, preventing the movement of fuel and other supplies.

An ice storm or blizzard can cause some disruption of or damage to IS facilities if outside equipment and the building are not designed to survive severe ice and snow accumulation. Off site, there may be widespread disruption of utilities and communications and roads may be dangerous or impassable.

The consequences of lightning strikes can range from no impact to disaster. The effects depend on the proximity of the strike and the efficacy of grounding and surge protector measures in place. Off site, there can be disruption of electrical power and there is the potential for fires.

Flooding is a concern in areas that are subject to flooding and for facilities that are in severe flood areas at low elevation. Damage can be severe, with long-lasting effects and the need for a major cleanup operation.

Besides Natural Disasters, there are local environmental threats that have to be considered. They may be grouped in six categories:

a. Inappropriate Temperature and Humidity

Computers and related equipment are designed to operate within a certain temperature range. Most computer systems should be kept between 10 and 32 degrees Celsius (50 and 90 degrees Fahrenheit). Outside this range, resources might continue to operate but produce undesirable results. If the ambient temperature around a computer gets too high, the computer cannot adequately cool itself, and internal components can be damaged. If the temperature gets too cold, the system can undergo thermal shock when it is turned on, causing circuit boards or integrated circuits to crack**.** Table 5.2 indicates the point at which permanent damage from excessive heat begins.

Another temperature-related concern is the internal temperature of equipment, which can be significantly higher than room temperature. Computer-related equipment comes with its own temperature dissipation and cooling mechanisms, but these may rely on, or be affected by, external conditions.

Such conditions include excessive ambient temperature, interruption of supply of power or heating, ventilation, and air-conditioning (HVAC) services, and vent blockage. High humidity also poses a threat to electrical and electronic equipment. Long-term exposure to high humidity can result in corrosion. Condensation can threaten magnetic and optical storage media. Condensation can also cause a short circuit, which in turn can damage circuit boards. High humidity can also cause a galvanic effect that result in electroplating, in which metal from one connector slowly migrates to the mating connector, bonding the two together

Table 5.2 Temperature thresholds for damage to computing resources

Component or Medium	Sustained Ambient Temperature at which Damage May Begin
Flexible disks, magnetic tapes, etc.	38 ° C
Optical media	49 ° C
Hard disk media	6 ° C
Computer equipment	79 ° C
Thermoplastic insulation on wires carrying hazardous voltage	125 ° C
Paper products	177 ° C

. Very low humidity can also be a concern. Under prolonged conditions of low humidity, some materials may change shape and performance may be affected. Static electricity also becomes a concern. A person or object that becomes statically charged can damage electronic equipment by an electric discharge. Static electricity discharges as low as 10 volts can damage particularly sensitive electronic circuits, and discharges in the hundreds of volts can create significant damage to a variety of electronic circuits. Discharges from humans can reach into the thousands of volts, so this is a nontrivial threat. In general, relative humidity should be maintained between 40% and 60% to avoid the threats from both low and high humidity.

Dealing with inappropriate humidity and temperature is a matter of having environmental-control equipment of sufficient capacity and appropriate sensors to warn of thresholds being exceeded.

b. Fire and Smoke

Perhaps the most frightening physical threat is fire. It is a threat to human life and property. The threat is not only from the direct flame but also from heat, release of toxic fumes, water damage from fire suppression, and smoke damage. Further, fire can disrupt utilities, especially electricity. Smoke damage related to fires can also be extensive. Smoke is an abrasive. It collects on the heads of unsealed magnetic disks, optical disks, and tape drives. Electrical fires can produce an acrid smoke that may damage other equipment and may be poisonous or carcinogenic. The most common fire threat is from fires that originate within a facility, and, as discussed subsequently, there are a number of preventive and mitigating measures that can be taken. A more uncontrollable threat is faced from wildfires, which are a plausible concern in the western United States, portions of Australia (where the term bushfire is used), and a number of other countries.

Dealing with fire involves a combination of alarms, preventive measures and fire mitigation such as:

- Choice of site to minimize fires originates from other regions,
- Designing the flow of air to prevent spreading the fire,
- Avoiding flammable materials inside the system center,
- Maintaining hand operated fire extinguishers available and regularly tested,
- Fire and Smoke detectors,
- Emergency procedures,
- Fireproof vaults for important printed documents,
- Disaster recovery backups of all systems stored off the premises,
- Inspection by insurance company and fire department.

c. Water Damage

Water and other stored liquids in proximity to computer equipment pose an obvious threat. The primary danger is an electrical short, which can happen if water bridges between a circuit board trace carrying voltage and a trace carrying ground. Moving water, such as in plumbing, and weather-created water from rain, snow, and ice also pose threats. A pipe may burst from a fault in the line or from freezing. Sprinkler systems, despite their security function, are a major threat to computer equipment and paper and electronic storage media. The system may be set off by a faulty temperature sensor, or a burst pipe may cause water to enter the computer room. For a large computer installation, an effort should be made to avoid any sources of water from one or two floors above. An example of a hazard from this direction is an overflowing toilet. Less common but more catastrophic is floodwater. Much of the damage comes from the suspended material in the water. Floodwater leaves a muddy residue that is extraordinarily difficult to clean up.

Prevention and mitigation for water threats involves plumbing leaks and other sources of water that causes flood. Exact locations of cut off valves should be documented to cut water supply in the event of a plumbing leak. Also water sensor should be located under the raised floor of computer rooms in order to cut off power in the event of a flood.

d. Chemical, Radiological, and Biological Hazards

Chemical, radiological, and biological hazards pose a growing threat, both from intentional attack and from accidental discharge. None of these hazardous agents should be present in an information system environment, but either accidental or intentional intrusion is possible. Nearby discharges (e.g., from an overturned truck carrying hazardous materials) can be introduced through the ventilation system or open windows and, in the case of radiation, through perimeter walls. In addition, discharges in the vicinity can disrupt work by causing evacuations to be ordered. Flooding can also introduce biological or chemical contaminants. In general, the primary risk of these hazards is to personnel. Radiation and chemical agents can also cause damage to electronic equipment.

e. Dust

Dust is a prevalent concern that is often overlooked. Even fibers from fabric and paper are abrasive and mildly conductive, although generally equipment is resistant to such contaminants. Larger influxes of dust can result from a number of incidents, such as a controlled explosion of a nearby building and a windstorm carrying debris from a wildfire. A more likely source of influx comes from dust surges that originate within the building due to construction or maintenance work.

Equipment with moving parts, such as rotating storage media and computer fans, are the most vulnerable to damage from dust. Dust can also block ventilation and reduce radiational cooling.

To prevent dust hazards proper air filtering should be used and a regular cleaning tasks should be done to prevent dust accumulation.

f. Infestation:

One of the less pleasant physical threats is infestation, which covers a broad range of living organisms, including mold[11], insects, and rodents[12]. High-humidity conditions can lead to the growth of mold and mildew, which can be harmful to both personnel and equipment. Insects, particularly those that attack wood and paper, are also a common threat. If these types of threats are present pest control procedures may be needed. Also a clean environment is very important.

5.6.2 Technical threats

This category encompasses threats related to electrical power and electromagnetic emission.

a. Electrical power

Electrical power is essential to the operation of an information system. All the electrical and electronic devices in the system require power, and most require uninterrupted utility power. Power utility problems can be broadly grouped into three categories: under voltage, overvoltage, and noise An under voltage occurs when the IS equipment receives less voltage than is required for normal operation. Under voltage events range from temporary dips in the voltage supply to brownouts (prolonged under voltage) and power outages. Most computers are

[11] Mold; is any fungi that cause disintegration of organic matter.

[12] Rodents; is a group of mammals, which includes rats, mice, squirrels, muskrats, beavers, and others.

designed to withstand prolonged voltage reductions of about 20% without shutting down and without operational error. Deeper dips or blackouts lasting more than a few milliseconds trigger a system shutdown. Generally, no damage is done, but service is interrupted. Far more serious is an overvoltage . A surge of voltage can be caused by a utility company supply anomaly, by some internal (to the building) wiring fault, or by lightning. Damage is a function of intensity and duration and the effectiveness of any surge protectors between your equipment and the source of the surge. A sufficient surge can destroy silicon-based components, including processors and memories. Power lines can also be a conduit for noise . In many cases, these spurious signals can endure through the filtering circuitry of the power supply and interfere with signals inside electronic devices, causing logical errors.

To deal with electrical problems uninterruptable power supply (UPS) units should be employed. They can protect systems from short power outages, power surges and electrical noise. For longer blackouts appropriate size of generators should be in place to supply UPS's.

b. Electromagnetic interference

Noise along a power supply line is only one source of electromagnetic interference (EMI). Motors, fans, heavy equipment, and even other computers generate electrical noise that can cause intermittent problems with the computer you are using. This noise can be transmitted through space as well as nearby power lines. Another source of EMI is high-intensity emissions from nearby commercial radio stations and microwave relay antennas. Even low-intensity devices, such as cellular telephones, can interfere with sensitive electronic equipment.

Dealing with electromagnetic interference is mainly applying combination of shields and filters. Specific technical details will depend on the infrastructure design and anticipated sources of electromagnetic interference.

5.6.3 Human-caused physical threats

Human-caused threats are more difficult to deal with than the environmental and technical threats discussed so far. Human-caused threats are less predictable than other types of physical threats. Worse, human-caused threats are specifically designed to overcome prevention measures and/or seek the most vulnerable point of attack. We can group such threats into the following categories:

a. Unauthorized physical access

Those who are not employees should not be in the building or building complex at all unless accompanied by an authorized individual. Not counting PCs and workstations, information system assets, such as servers, mainframe computers, network equipment, and storage networks, are generally housed in restricted areas. Access to such areas is usually restricted to only a certain number of employees. Unauthorized physical access can lead to other threats, such as theft, vandalism, or misuse.

b. Theft

This threat includes theft of equipment and theft of data by copying. Eavesdropping and wiretapping also fall into this category. Theft can be at the hands of an outsider who has gained unauthorized access or by an insider. To prevent theft tracking devices can be placed on mobile equipment.

c. Vandalism

This threat includes destruction of equipment and destruction of data.

d. Misuse

This category includes improper use of resources by those who are authorized to use them, as well as use of resources by individuals not authorized to use the resources at all.

6. SECURITY RISK MANAGEMENT

6.1 General

Risk management is the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations' missions. The head of an organizational unit must ensure that the organization has the capabilities needed to accomplish its mission. These mission owners must determine the security capabilities that their IT systems must have to provide the desired level of mission support in the face of real world threats. Most organizations have tight budgets for IT security; therefore, IT security spending must be reviewed as thoroughly as other management decisions. A well-structured risk management methodology, when used effectively, can help management identify appropriate controls for providing the mission-essential security capabilities as stated by NIST [16].

In general, a risk exists when there is a possibility of a threat to exploit the vulnerability of a valuable asset. That is, three elements of a risk are: asset, vulnerability and threat. The value of as asset makes it a target for an attacker. The vulnerability of an asset presents the opportunity of a possible asset damage or loss. A threat is a potential attack which can exploit a vulnerability to attack an asset as noted by Ye [17].

Security risk assessment and management are essential for effective security engineering. Risk management is concerned with assessing the possible losses that might ensue from attacks on assets in the system and balancing these loses against to cost of security procedures that may reduce these losses.

Risk management is a business issue rather than a technical issue, so software engineers or system administrators should not decide what controls should be included in a system. It is up to senior management to decide whether or not to accept the cost of security or to accept the exposure that results from the lack of security procedures. However the role of the technical staff is to provide informed technical guidance and judgments on security issues. They are, therefore, essential participants in the risk management process as noted by Sommerville [12].

As noted by Sommerville [12] a critical input to risk assessment and management process is the organizational security policy. An organizational security policy applies to all systems and should set out what should and what should not be allowed. For example one aspect of military security policy may state 'Readers may only examine documents whose classification is the same as or below the reader's vetting level'. This means that if a reader has been vetted to a 'secret' level, they may access to documents that are classed as 'secret', 'confidential', or 'open' but not documents classed as 'top secret'. The security policy sets out conditions that should always be maintained by a security system an so helps identify threats that might arise. Risks are anything that could threaten business security. In principle, security policies can be stated formally and various automated checks made against them. In practice, they are normally informal documents that what is and what is not allowed.

6.2 Preliminary Risk Assessment

The objective of preliminary risk assessment is to derive the security requirements for whole system, not just software. These influence the choice of the system platform and middleware and serve as basis for developing more detailed software functional requirements.

The essential stages of preliminary risk assessment are given by Sommerville[12] as follows

a. Asset identification where the system assets that may require protection are identified. The system itself or particular system functions may be identified as assets as well as the data associated with the system.
b. Asset value assessment where you estimate the value.
c. Exposure assessment where you assess the potential losses associated with each asset.
d. Threat identification where you identify the threats to system assets.
e. Probability assessment where you estimate the probability of each threat.

f. Control identification where you propose the controls that might be put in place to protect an asset.
g. Feasibility assessment where you assess the technical feasibility and the costs of proposed controls
h. Security requirements definition where the exposure, threats and control assessments are used to derive a set of system security requirements. These may be requirements for the system infrastructure or the application system.

6.3 Life Cycle Risk Assessment

Security risk assessment should be part of all life cycle activities from requirements engineering to system deployment in software engineering and administration of system infrastructure. The process followed is similar to the preliminary risk assessment process with the addition of activities concerned with vulnerability identification and assessment. Vulnerability assessment identifies the assets that are likely to be affected by that vulnerability and relates these vulnerabilities to a possible system attacks. The outcome of risk assessment is a set of engineering decisions that affect the system design or implementation or limit the way in which it is used as noted by Sommerville[12].

Besides the environmental and technical threats, remaining part is caused by humans. These human threats and resulted attacks are mostly driven by some motive. NIST [16] describes motivation behind the threats and possible attack types that can occur in the Table 6.1 below

Once vulnerabilities have been identified, you then have to make a decision on what steps that you can take to reduce the associated risks. This will often involve making decisions about additional system security requirements or the operational process of using the system.

Security information and event managements tools assists risk assessment process by giving more in depth look to the relevant events that are recorded by various applications and security measures. This kind of tools, provide real world information to risk assessment processes and increases the validity of assessments.

Table 6.1 Human threats to information systems.

Threat Source	Threat Motivation	Action
Hacker, cracker	Challenge Ego Rebellion	• Hacking • Social engineering • System intrusion, break-ins • Unauthorized system access
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	• Computer crime (e.g., cyber stalking) • Fraudulent act (e.g., replay, impersonation, interception) • Information bribery • Spoofing • System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge	• Bomb/Terrorism • Information warfare • System attack (e.g., distributed denial of service) • System penetration • System tampering
Industrial espionage	(companies, foreign governments, other government interests) Competitive advantage Economic espionage	• Economic exploitation • Information theft • Intrusion on personal privacy • Social engineering • System penetration • Unauthorized system access (access to classified, proprietary, and/or technology-related information)
Insiders (poorly trained, terminated employees) negligent, dishonest, or disgruntled, malicious,	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g., data entry error, programming error)	• Assault on an employee • Blackmail • Unauthorized system access
		• Computer abuse • Fraud and theft • Information bribery • Input of falsified, corrupted data • Interception • Malicious code (e.g., virus, logic bomb, Trojan horse) • Sale of personal information • System bugs • System intrusion • System sabotage

6.3.1 Penetration testing and vulnerability assessment

Vulnerability is a weakness that can be exploited to gain access to that system. There are any number of ways that a system can be compromised: through poor password selection, viruses or Trojans, software bugs, an executable or script running inside the system, or through code injection. When a vulnerability becomes known and is used by others to attack similar systems, it is referred to as an exploit. Exploits travel as quickly as viruses do.

All software contains bugs or routines that can be compromised. The patches that companies offer on a regular basis, such as Microsoft Update, are meant to remove these vulnerabilities once they are discovered. When patches are released, they are analyzed for the flaws that they are meant to fix by people interested in attacking systems. An attack based on that flaw is then rushed out, and is very effective because it takes a while for systems to be updated. To uncover vulnerabilities vulnerability scanners can be used. Vulnerability scanners work by scanning a network for all assigned IP addresses, determining which ports are open, and building a list of applications and operating systems that are running on the various systems. Scanners of this type are port scanners, network scanners, and Web site scanners, as well as dedicated tools contained in management frameworks. Once the initial survey is complete, the scanner may either build a map of the network or create a report. If the scanner uses SNMP, WMI, or another management protocol, it can query systems and applications to determine not only what they are, but also their version numbers and patch levels. Vulnerability ratings can be assigned that provide administrators with check lists for actions that they need to perform in order to secure their network further as noted by Sosinsky [18].

An industry standard for measuring the severity of computer system vulnerability is called the Common Vulnerability Scoring System (CVSS). This metric is based on a set of measurements, and includes base or intrinsic vulnerability, perceived threats over time or temporal metrics, and deployment or environmental metrics. For more information on how this scoring system is structured, one can go to the CVSS FIRST (Forum of Incident Response and Security Teams) Web site at www.first.org/cvss/. The CVSS Special Interest Group, or SIG, develops this standard, which is currently at version 2. The metrics can be entered into an online calculator provided by the National Vulnerability Database in the CVSS scoring section to obtain the specific ratings as noted by Sosinsky [18].

Penetration testing is security testing in which evaluators attempt to circumvent the security features of a system based on their understanding of the system design and implementation. The purpose of penetration testing is to identify methods of gaining access to a system by using common tools and techniques used by attackers. Penetration testing should be performed after careful consideration, notification, and planning.

- Penetration testing can be an invaluable technique to any organization's information security program. However, it is a very labor-intensive activity and requires great expertise to minimize the risk to targeted systems. At a minimum, it may slow the organization's networks response time due to network scanning and vulnerability scanning. Furthermore, the possibility exists that systems may be damaged in the course of penetration testing and may be rendered inoperable, even though the organization benefits in knowing that the system could have been rendered inoperable by an intruder. Although this risk is mitigated by the use of experienced penetration testers, it can never be fully eliminated. Since penetration testing is designed to simulate an attack and use tools and techniques that may be restricted by law, federal regulations, and organizational policy, it is imperative to get formal permission for conducting penetration testing prior to starting. This permission, often called the rules of engagement, should include: NIST [19]
- Specific IP addresses/ranges to be tested
- Any restricted hosts (i.e., hosts, systems, subnets, not to be tested)
- A list of acceptable testing techniques (e.g. social engineering, DoS, etc.) and tools (password crackers, network sniffers, etc.)
- Times when testing is to be conducted (e.g., during business hours, after business hours, etc.)
- Identification of a finite period for testing

- IP addresses of the machines from which penetration testing will be conducted so that administrators can differentiate the legitimate penetration testing attacks from actual malicious attacks
- Points of contact for the penetration testing team, the targeted systems, and the networks + Measures to prevent law enforcement being called with false alarms (created by the testing)
- Handling of information collected by penetration testing team.

6.3.2 Security information and event management (SIEM)

As noted by Vacca[2], Security monitoring involves real-time or near-real-time monitoring of events and activities happening on all your organization's important systems at all times. To properly monitor an organization for technical events that can lead to an incident or an investigation, usually an organization uses a Security Information and Event Management (SIEM) and/or log management tool. These tools are used by security analysts and managers to filter through tons of event data and to identify and focus on only the most interesting events. Understanding the regulatory and forensic impact of event and alert data in any given enterprise takes planning and a thorough understanding of the quantity of data the system will be required to handle. The better logs can be stored, understood, and correlated, the better the possibility of detecting an incident in time for mitigation. In this case, what you don't know will hurt you. Responding to incidents, identifying anomalous or unauthorized behavior, and securing intellectual property has never been more important. Without a solid log management strategy it becomes nearly impossible to have the necessary data to perform a forensic investigation, and without monitoring tools, identifying threats and responding to attacks against confidentiality, integrity, or availability become much more difficult. For a network to be compliant and an incident response or forensics investigation to be successful, it is critical that a mechanism be in place to do the following:

- Securely acquire and store raw log data for as long as possible from as many disparate devices as possible while providing search and restore capabilities of these logs for analysis.

- Monitor interesting events coming from all important devices, systems, and applications in as near real time as possible.
- Run regular vulnerability scans on your hosts and devices and correlate these vulnerabilities to intrusion detection alerts or other interesting events, identifying high-priority attacks as they happen and minimizing false positives.

SIEM solutions in general can assist in security information monitoring as well as regulatory compliance and incident response by:(Vacca [2]),

- Aggregating and normalizing event data from unrelated network devices, security devices, and application servers into usable information.
- Analyze and correlate information from various sources such as vulnerability scanners, IDS/IPS, firewalls, servers, and so on, to identify attacks as soon as possible and help respond to intrusions more quickly.
- Conduct network forensic analysis on historical or real-time events through visualization and replay of events.
- Create customized reports for better visualization of your organizational security posture.
- Increase the value and performance of existing security devices by providing a consolidated event management and analysis platform
- Improve the effectiveness and help focus IT risk management personnel on the events that are important.
- Meet regulatory compliance and forensics requirements by securely storing all event data on a network for long-term retention and enabling instant accessibility to archived data.

7. DESIGN FOR SECURITY

7.1 General

The Internet has also driven the growth of security standards and technologies. Software vendors provide feature-rich security solutions and components at a level of complexity and maturity beyond almost all projects. Building one's own components is rarely an option, and security architecture work is primarily integration work. In today's environment, the emerging dominance of vendor products aiding software development for enterprise security cannot be ignored. One interacts with vendors on many levels, and our understanding of their product offerings depends on a combination of information from many sources: marketing, sales, customer service support, vendor architects, and other applications with experience with the product.(Ramachadran [20]).

7.2 Design Guidelines

There are no hard and fast rules about how to achieve system security. Different types of system require different technical measures to achieve a level of security that is acceptable to system owner. The attitudes and requirements of different groups of users profoundly affect what is and is not acceptable. For example, in a bank, users are likely to accept a higher level of security and hence more intrusive security procedures than in a university.

Also in software design is important for the overall security. UMLsec can be given as an example. The idea of UMLsec is to specify security at each level such that if the security specifications at each level are fulfilled by the next, more specific, level then result be secure as specified Braude and Berstein [21].

7.3 Architectural Design

In designing a system architecture that maintains security, you need to consider two fundamental issues:

1. **Protection** – how should the system be organized so that critical assets can be protected against external attack.
2. **Distribution** – how should system assets be distributed so that the effects of a successful attack is minimized.

These issues are potentially conflicting. If you put all your assets in one place, then you can build layers of protection around them. However, if that protection fails, then all your assets are compromised. On the other hand, if you distribute assets, they are more expensive to protect and the chances are greater that the protection will be breached. However, if this happens you do not suffer a total loss.

In order to provide protection in a system, one normally uses a layered architecture with the critical protected assets at the lowest level in the system and with various layers of protection around them. These layers are:

1. **Platform-Level Protection:** The top level controls access to the platform on which the patient record system runs. This usually involves a user signing-on to particular computer. The platform will also normally include support for maintaining the integrity of files on the system.
2. **Application Level Protection:** The next protection level is built into application itself. It involves a user accessing the application, being authenticated and authorized to take actions such as view or modify data.
3. **Record-Level Protection:** This level invoked when access to specific records is required and involves checking that a user is authorized to carry out the requested operations on that record. Protection at this level is might also involves encryption to ensure the records cannot be browsed by a file browser. Integrity checking using, for example, cryptographic checksums can detect changes that have been made outside the normal record update mechanisms.

The number of protection layers that you need in any particular application depends on the criticality of the data. Not all applications need protection at the record level and coarser-grain access control is more commonly used. To achieve security, you should not allow the same user credentials to be used at each level. If protection of data is a critical requirement, than a client-server architecture should be used, with the protection mechanisms built into server. However, if the protection is compromised, then the losses associated to the attack are likely to be high, as are the costs of recovery.

A problem that can arise when designing a secure system is that the architectural style that is most appropriate for providing security may conflict with other application requirements. For example, say an application has an absolute requirement to maintain the confidentiality of a large database and requirement for very fast access to that data. Satisfying these, in the same architecture, can be difficult. A high level of protection suggests that layers of protection are required. This is an inevitable performance overhead, thus slowing down access to the data. If an alternative style is used, then implementing protection and guaranteeing confidentiality may be more difficult and expensive.

7.4 Logical and Physical Architecture

As one conducts security assessments, it is imperative to enumerate all necessary architectural elements needed to develop the target security architecture. The recommendations can be used to make necessary architectural changes to existing IT infrastructure design, implementations, and policies and to add security controls to other architectures. It is important to develop two types of security architecture designs (Farah [22]):

- **A logical architecture** of IT security components is needed to organize the physical architecture and implement security in all identified architectures. The logical structure includes processes, technology and people. It consists of perimeter security, a computer incident response team, antivirus policy, security administration, a Disaster Recovery Plan (DRP), risk and threat analysis, data security, application security, and infrastructure security.

- **Physical architecture** designs include network diagrams illustrating firewalls, mail gateways, proxies, modem pools, VLANs, Demilitarized Zone (DMZ), internal and external connections and devices used, and diagrams of other architectures in relation to security architecture.

7.5 Defense in Depth

As noted by Daswani et al.;[23] the point of defense-in-depth is to not rely on any one defense to achieve security. Multiple mechanisms can help you achieve more security than just one. Some mechanisms (such as the security guards outside the bank) might help prevent attacks. In the case of a bank robbery, it is usually quite obvious when the robbery is taking place—but in the world of network security, it may not even be clear when an attack is taking place. As such, some mechanisms might help you detect when attacks are taking place. Since it is not always possible to prevent attacks all together, it is important to deploy mechanisms that help you manage or contain attacks while they are in progress. In some banks, bank tellers are stationed behind bulletproof glass, which helps contain the effect of a bank robbery by working to spare the lives of the bank tellers in the case that violence breaks out. After an attack takes place, you want to be able to recover from the attack, to whatever extent possible. Bank tellers may give the robbers a specially prepared briefcase of cash that will spurt dye on the robber when he opens it. The police will then be able to find the bank robber because the dye can only be removed using special chemicals, which helps create accountability. In addition to dye-laced briefcases, banks takeout insurance policies to help deal with the financial loss in case the cash cannot be recovered. A good security system, whether it to be physical security of banks or software information systems, should employ defense-in-depth, and include mechanisms that help to prevent, detect, manage, and recover from attacks (NASA [24]).

Most security experts would agree with the view that perfect network security is impossible to achieve and that any single defense can always be overcome by an attacker with sufficient resources and motivation. The basic idea behind the defense-in-depth strategy is to hinder the attacker as much as possible with multiple layers of defense, even though each layer might be surmountable. More valuable assets are protected behind more layers of defense. The combination of multiple layers increases the cost for the attacker to be successful, and the cost is proportional to the value of the protected assets. Moreover, a combination of multiple layers will be more effective against unpredictable attacks than will a single defense optimized for a particular type of attack. The cost for the attacker could be in terms of additional time, effort, or equipment. For instance, by delaying an attacker, an organization would increase the chances of detecting and reacting to an attack in progress. The increased costs to an attacker could deter some attempts if the costs are believed to outweigh the possible gain from a successful attack.

Defense in depth is sometimes said to involve people, technology, and operations. Trained security people should be responsible for securing facilities and information assurance. However, every computer user in an organization should be made aware of security policies and practices. Every Internet user at home should be aware of safe practices (such as avoiding opening email attachments or clicking suspicious links) and the benefits of appropriate protection (antivirus software, firewalls).

A variety of technological measures can be used for layers of protection. These should include firewalls, IDSs, routers with ACLs, antivirus software, access control, spam filters, and so on. The term operation refers to all preventive and reactive activities required to maintain security. Preventive activities include vulnerability assessments, software patching, system hardening (closing unnecessary ports), and access controls. Reactive activities should detect malicious activities and react by blocking attacks, isolating valuable resources, or tracing the intruder. Protection of valuable assets can be a more complicated decision than simply considering the value of the assets. Organizations often perform a risk assessment to determine the value of assets, possible threats, likelihood of threats, and possible impact of threats. Valuable assets facing unlikely threats or threats with low impact might not need much protection. Clearly, assets of high value facing likely threats or high-impact threats merit the strongest defenses. Organizations usually have their own risk management process for identifying risks and deciding how to allocate a security budget to protect valuable assets under risk.

8. AN APPLICATION

8.1 General

As mentioned in previous chapters IS security of an organization include various type of efforts. In order to achieve the desired security levels all of these issues should be handled by the relevant group of people. Due to the complexity of such process, in this thesis an application will be developed to demonstrate the technical part of logical security in IS security.

The proposed application aims to improve the logical security architecture of an organization. Every organization differs from each other according to the environment it operates, needed infrastructure and desired level of security. Such as, a military organization will need confidentiality more rather than availability. Because the information residing inside the system is secret and it should be remain secret rather than available. In contrast to this example, a hospital needs their systems available and intact all the time but even if the information they carry is confidential, it is not important in the condition that the systems are not working and the doctors can't work. Besides the security point of view every type of organization uses different types and amounts of information technologies to operate and also some will expose their services to internet and others don't. Also it is assumed that the information this application will develop upon is secret for an actual organization. It is clear that finding an organization to willingly share this type of information is very hard and in the case of some organization is to share this information, discussing this type of information in public is unethical.

Regarding the confidentiality issues and diversity of organizational needs the proposed application will define a fictitious organization and apply all the security elements on it. At first sight it will look as an overkill application of all security products without looking into what is needed and what is not, but the aim is to recommend an architecture to deploy infrastructural security products and also show how they work together to protect assets.

8.2 Definition of a Fictitious Organization

In order to define a sample organization one should first decide which aspects are necessary for the definition. For example, geographical location of a data center is important if one is considering assessing physical security issues but it is not important in this application because the logical architecture of the organization is going to be examined. In order to define the organization as simple as possible, answers to the following questions below will be used:

1. Is it a private or governmental organization?
2. How many internal users are present?
3. Is there any service exposed to internet?
4. How important confidentiality, integrity and availability to the organization?
5. How many external users are present? And how often do they use it?
6. Is there any remote office(s)?
7. Is there any mobile internal users?

Answers of these questions may reveal some properties of the proposed fictitious organization for application development. In the application; following properties of the fictitious organization are chosen in the Table 8.1.

Table 8.1 Properties of the fictitious organization

Property	Value
Type of the organization	Government
Number of Internal Users	3000+
Services over Internet	Yes
Security Categorization	High
Number of External Users	1 Million+
Remote Offices	Yes
Mobile Users	Yes

This organization provides a web service that external users use to apply some forms and see their related personal information about organizations. There is also reported incidents that high load of traffic makes services unavailable in various conditions. The nature of this traffic pattern is not known clearly whether It is normal or malicious. Three tiered architecture is used to develop the IS application, consisting of a web frontend, an application server and a database server.

According to the security categorization previously mentioned organization is ranked high because this governmental organization has high confidentiality, integrity and availability impact. There is information about citizens on the databases that have to remain secret. Also the service given is crucial to day to day activities of the people and must be available all the time. Records of citizens are used by this and other government agencies as a national data, therefore integrity of the records are highly important.

As seen in the Figure 8.1, corporate network infrastructure consists of Demilitarized Zone (DMZ), server and client segments. DMZ as a military term is a zone or a buffer area between two militarized sides where military activity is forbidden by an agreement. In networking this term used for a network segment. This segment separates and acts as a buffer between internet and internal network. Aim is to place services that are exposed to internet there and separate from the internal network. According to this, DMZ is a particular network which is in between trusted (internal network) and untrusted (internet) networks to acts as a intermediate space. Typically this segment hosts mail, web and dns[13] servers. Other servers that are exposed to internet can be placed here regardless of this example organization.

Client workstations, wireless access points, printers and other IP enabled devices are connected to corresponding floor switch in network connected devices segment. Figure 8.1 and other figures in this application are logical in nature. For example there are additional physical connections before the floor switches but

[13] DNS; is a protocol used by domain name services to translate numerical addresses for host names.

they are not shown here to simplify the figure. Floor switches aggregates at the backbone switch to maintain access to internet and other internal networks.

Server segment contains all the internal servers. The server switch aggregates all servers and connects to the backbone. As stated earlier there can be additional physical connections to meet the bandwidth requirements of the server segment but they are not shown in the figure.

There are also remote offices which access organization through internet. Communication is done with explicit rules on the firewall to permit access and no network level encryption is used for communication confidentiality. External users access the web services from the internet.

Host based security products such as antivirus software and host intrusion prevention software are installed locally and management of these products from a single point is not available. There is no visibility of whether these products installed or up to date for recent signatures.

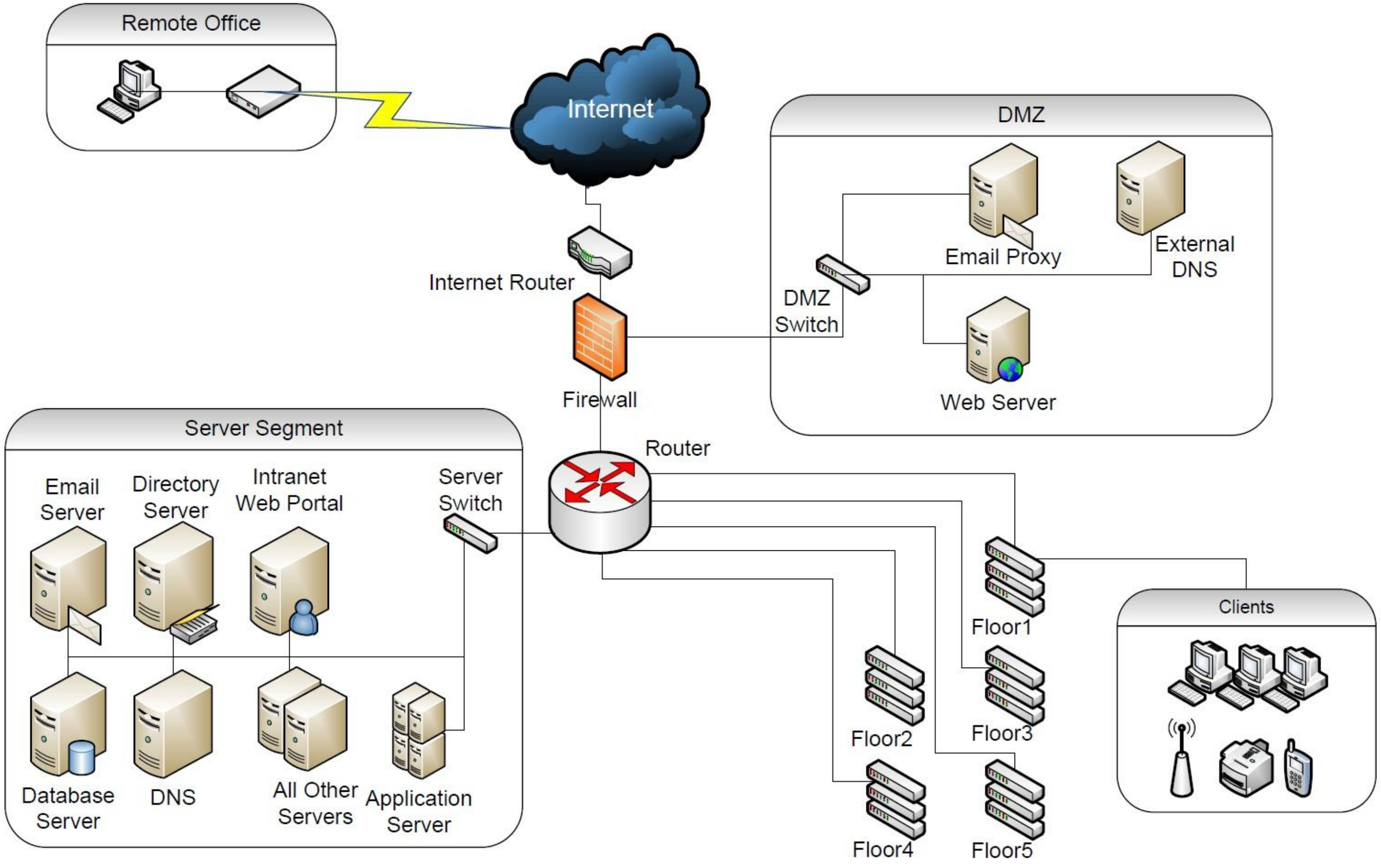


Figure 8.1 Organization network infrastructure.

9. APPLICATION DEVELOPMENT

9.1 Introduction

Defined fictitious organization has disadvantages regarding IS security. They can be simply stated as:

- Controlling the access of internal networks to the servers can only be enforced from the backbone switch. This should be done on a proper firewall with additional capabilities such ad user authentication and granular configuration.
- There is a single security element as a first line of defense which is a firewall. A firewall can only prevent or grants access to certain ports. Today there are numerous attacks that use well known and permitted ports on firewalls.
- There is no preventive or protective measure against malware threats.
- Remote connections security is not maintained at all times. If used application does not support encryption, traffic passing is unencrypted and vulnerable to eaves dropping.
- There is no proper load balancing mechanism to keep services working under heavy load or a way to increase the number of servers.
- There is no redundant networking which causes network downtime if an appliance goes out of order.
- There is no dedicated security for web applications or databases

This assessment considers most general problems that every typical organization faces and there can be additional items if an actual organization is considered. These issues will be handled in the resulting architecture.

Information systems made up of a network and computers that communicates inside this network. Some part of this network is internet which external users way to communicate. In this application internal network of the defined organization will redesigned to achieve a more secure IS.

Main regions of the organization network can be divided into four parts.

1. Perimeter Network
2. Core Network
3. Local Area Network
4. Wide Area Network

By this type of grouping network segments can be split into more manageable parts. Communication between them can be seen at the Figure 9.1.

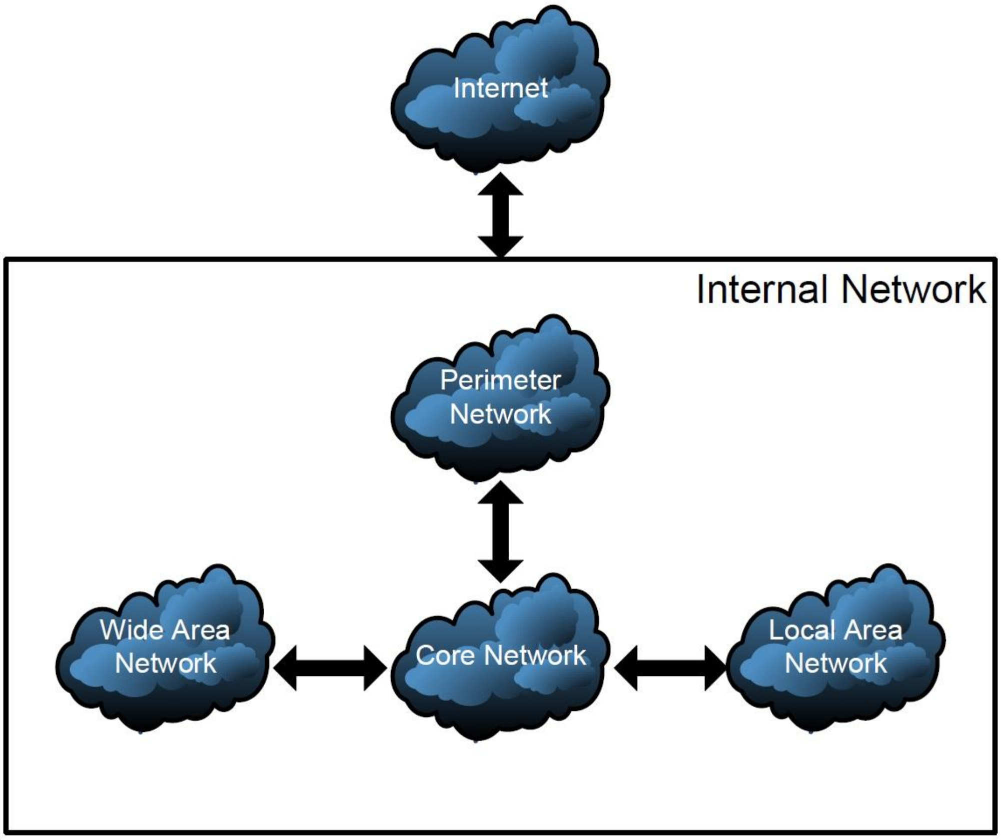


Figure 9.1 Internal network.

Simple definitions for these segments are given below:

Perimeter Network: Is the most outer layer of the network infrastructure. It is a general definition that houses DMZ segment and the security devices that separates it from other internal networks.

Core Network: Is the core of the network. It is the central communication point of neighbor networks with each other. It hosts the internal servers and security products for clients.

Local Area Network: Client workstations and other network supported devices such as printers and smart phones are at this segment. In order to communicate with the internet and internal servers, this segment is communicates with the core network.

Wide Area Network: It is the remote offices that are connected through public networks to the organization.

The details of these segments will be given in detailed figures. At first these figures may seem to show physical connections because of the physical elements used but the connection between the elements are in logical manner. This type of illustration is used to maintain a more simple view of the arrangement of devices. Cabling of the devices may vary on an actual installation.

Networking infrastructure is made redundant on all segments. Redundancy in networking means that there is more than one path to reach to the destination. When the network is not redundant any network device that is faulty can cause network downtime. This results a single point of failure, which is the fail of the whole path with one element. In order to avoid this network level security devices should be redundant as well as the networking devices such as routers or switches.

When networks do not have single failure points their risk of network interruption is reduced and also availability of the services are increased accordingly.

9.2 Perimeter Network

Security devices used in this network is:

1. Intrusion Prevention System
2. Firewall
3. Antivirus-Antispam Server
4. Load Balancer

As seen in Figure 9.2 Firewall placement is not changed according to the original organization definition but because of the redundant network cluster firewalls added. This ensures that traffic in each line is passing through a firewall. In the event of a firewall failure, other identical device can operate and do not interrupt the network traffic. DMZ segment is separated by the external firewall from other internal network zones. Servers that are exposed to the internet are placed in this zone and this zone should not contain any client devices or servers that have private data. This type of placement ensures that only the needed systems are directly exposed to internet and keep other systems out of reach.

Intrusion prevention systems are added in front of the servers and internet facing side of the firewall. IPS's are used to detect attacks based on attack signatures. They have statistical methods to profile normal amount of traffic to prevent some attacks such as Denial of service or DoS in short. Network IPS devices are deployed as in line mode. This means that the traffic is passing through the devices and inspected on wire speed. The ports of the IPS are not sensed by other devices on the network because they don't have any IP. This results a total transparent deployment and no need to change any network configuration.

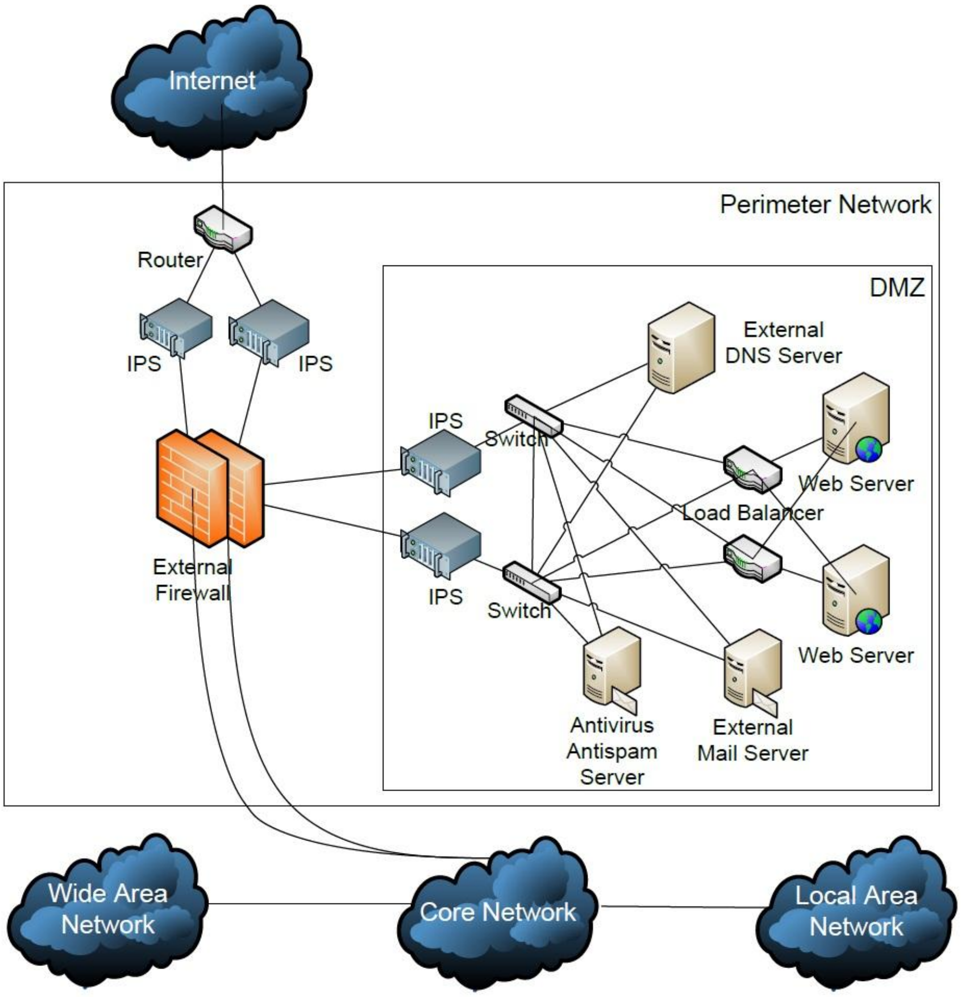


Figure 9.2 Details of the perimeter network

In perimeter network IPS devices are positioned to inspect traffic passing through

- Between firewall and Internet
- Between firewall and Servers

Internet side IPS protects the firewall from DoS attacks and acts as a first line of defense. At the servers part IPS serve as a protection against the internal users. This will prevent an attacker that has gained an access to an internal client machine or server to attack the perimeter network servers from inside.

Figure 9.2 shows four IPS figures to inspect related connections but there are two IPS devices are used in physical configuration. One network IPS device has a number of ports to inspect traffic according to its size. High capacity IPS devices have ports enough to monitor large number of network lines. Selecting an IPS device depends on how many network segments are going to be monitor and how much traffic will be passing through one device. Appropriate size devices should be used but this not the scope of this application.

Antivirus-Antispam server is a security product that inspects emails for spam and malicious content or malware. From now on it is mentioned as antispam servers because its main purpose is to prevent spam. Antispam server can be positioned as a gateway device that passes all the traffic on the line or can be configured as a proxy server. Because antispam servers only inspect mail, proxy mode is chosen to prevent other unrelated traffic to pass through the device. It is connected like any other server and accepts SMTP connections to inspect mail coming from outside. Appropriate network translation rules are applied to send all the incoming mail to the antispam server for inspection. After the inspection completed antispam server forwards the mail to external mail server. Also it prevents malware that is attached to mails by simple antivirus scanning and also blocks mail threats such as phishing attacks. Outgoing mails can also send and inspected through the device. If certain amount of spam mail originates from the organization the mail IP can be added to the spam blacklists. This will cause organizations legitimate mails to be blocked by other antispam servers.

Load balancer devices are essentially not security oriented devices but they support the availability of the systems. Because of the high amounts of traffic mentioned in the organization definition a load balancer and an extra web server is added to the perimeter network. Two load balancers are used to support redundant networking and to prevent single point of failure. Load balancers can also terminate SSL sessions to reduce the CPU usage of the web servers. This is often called as SSL offloading.

Load balancing methods are different and they have extra abilities such as checking the health of the services before sending traffic but the configurations are not defined in this application because the configuration of the load balancer will depend on the conditions of the situation.

9.3 Core Network

Core network is the central part of the whole network of the organization. Security devices used in this network can be divided in to two groups

1. Security for Clients
    - URL Filter
    - Gateway Antivirus
    - Gateway Data Loss Prevention
    - Caching Proxy
    - Content Redirection Switch

2. Security for Servers
    - Web Application Firewall
    - Database Firewall
    - IPS
    - Load Balancer.

Figure 9.3 shows the details of the core network. The arrangement of the devices is changed to provide more compartmentalized architecture. By this architecture there is ability to integrate infrastructural security products easily and if needed further expansion of the network is feasible.

Communication center is replaced from backbone to an internal firewall. This provides ability to control access to several network segments in one point. Local area network and wide area network are connected through the internal firewall. In order to support the redundant network, cluster firewall is used as an internal firewall. Resulting structure clearly divides the internet , perimeter network and the other internal networks.

9.3.1 Security products for clients

When a client access to internet, as shown in Figure 9.3, travels the through internal firewall, content redirection switch and perimeter network respectively. Content redirection switch plays an important role in this path because it redirects some traffic no security devices for inspection and approval. Example of the protocols used in this redirection can be HTTP or FTP. Traffic is redirected to following devices:

1. **URL filter:** Simply URL filters are devices that block http connections according to the requested URL. Except military organizations, many organization allows users to browse web unrestricted and it brings problems with it. Malware threat and excessive usage of bandwidth is two major ones. In order to prevent these threats user access to malicious sites are prevented by URL filters. Also blockings are configured according to the internet usage policy of the organization. By preventing the users to visit sites that spread malware, a preventive measure is taken against the malware problem.

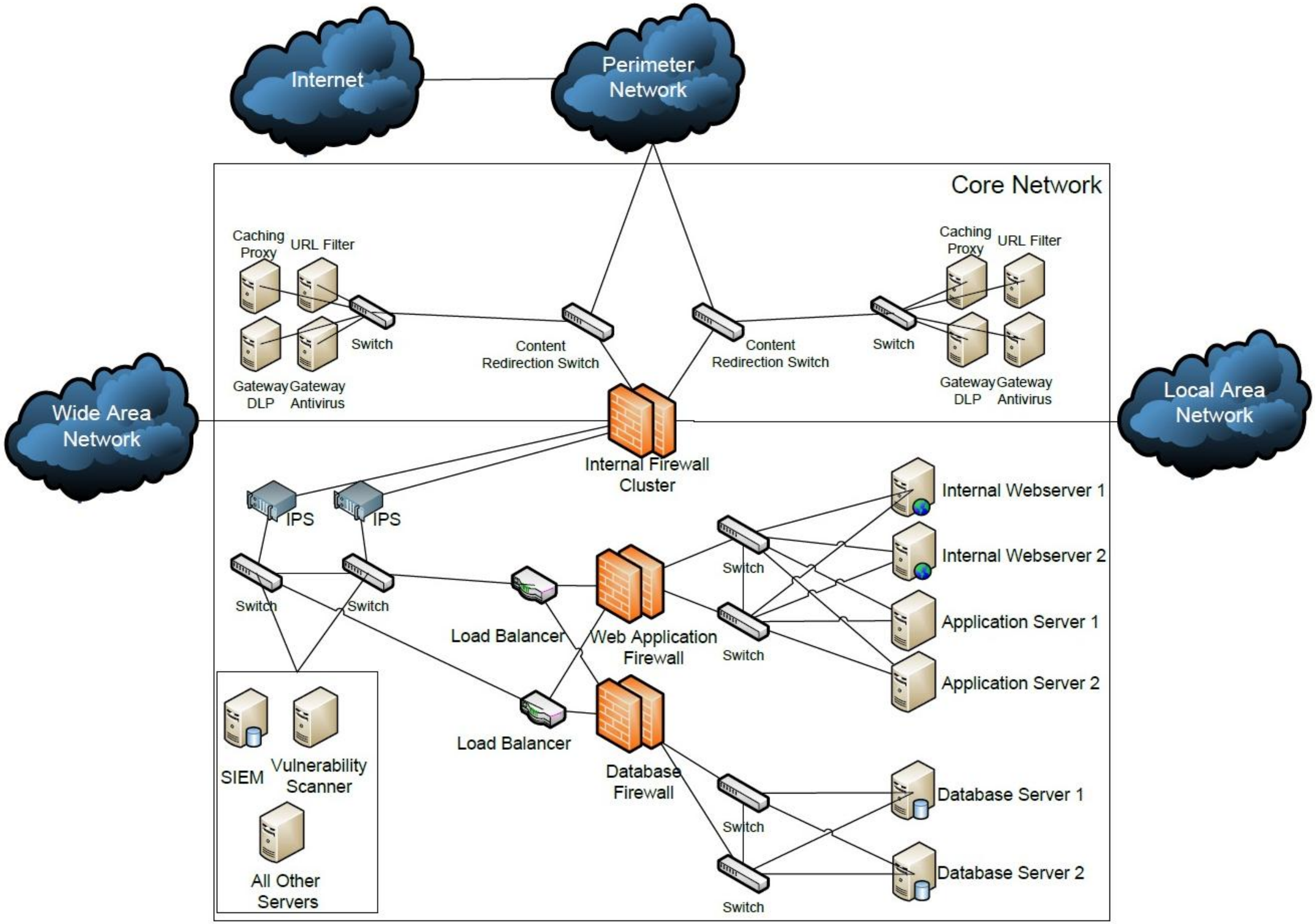


Figure 9.3 Details of the core network

2. **Gateway antivirus:** Gateway antivirus devices scan the relevant traffic for malware.. This supports the preventive function of URL filters. If any malware site that is not blocked from the site sends a malware, gateway antivirus will effectively block the file. This protective approach provides stopping the malware at the network layer before it reaches the clients. Types of protocols can be inspected varies from a vendor to another and because of that details of the traffic redirected is not given in this application.
3. **Gateway data loss prevention:** DLP systems monitor the sensitive data which is travelling through the network. In the case of violation DLP systems can terminate the connection and collect evidence for further inspection. DLP systems plays an important role on recent days, leakage of information is common and a major threat to organizations information confidentiality. Placing at the network where all client to internet communication takes place, provides organization more insight to the sensitive data going out of the internal network.
4. **Caching proxy:** Caching proxy servers are used to cache repetitive web traffic of internal users. By using caching organization saves the internet bandwidth to more important functions and improve availability of services.

By using all these security products internet traffic of local users are deeply inspected for malware and sensitive data. Usage of content redirection switches gives the ability to do redirection without making any configurations on the user systems.

In order support redundant network two sets of devices are used for each network path.

9.3.2 Security products for servers

When security of servers are considered an effective control of access and an IPS system seems to enough but today web based attacks are very common. Also majority of organizations like our fictitious one give web services to the internet. This situation brings the need to take extra security precaution on web applications. Regardless of this an IPS device is placed on the network line where the servers are connected to internal firewall(Figure 9.3). This deployment of IPS provides protection of all servers because any traffic passing through to the servers segment is inspected.

In order to secure web applications and related components, as seen in Figure 9.3, there are additional security products are used.

Web application firewall: inspect the HTTP traffic on the line. They are very much alike IPS devices but more sophisticated according to them. Web application firewalls protect web applications from attacks such as SQL injection. Many of these attacks exist because of the development mistakes of the software. For example SQL injection is done by sending an SQL query with a field or URL and executing wrongly on the database server. Injection attacks can be effectively prevented if user input validations are in place but this type of mistakes can only be noticed after some incident really occur. For critical systems there is no margin for a mistake like this to be exploited. There for Web application firewalls monitors application layer traffic and prevent attacks when they are detected. Besides the attack detection web application firewalls keep track of user inputs to the web service and can learn the normal usage of the application. It can learn that some form fields are number only or some fields can' be larger than a specified length. After learning process, with the help of the software development team, prevention of unwanted entries can be configured.

Database firewall: is similar to web application firewalls. They inspect remote database calls in the application layer. In order to web application function correctly queries that are needed to run on the database are permitted. Any query other than these one will generate an alert for further inspection. Risky sql keywords such as Delete or truncate can be forbidden to some users to prevent accidental data loss. Authorized users can be designated for executing such queries. Database firewalls also protect the database application. For example there are attacks specific for an Oracle database. These devices have attack definitions on them to prevent when such a threat against the database application is present.

Some vendors provide a feature that is very useful to investigate issues: web user tracking on database operations. Commonly web applications designed for logging in to database with a predefined user. After a user is authenticated at the front end their insert or select operations performed by the web application which uses a single database user. Hence, tracking the user operations on databases becomes impossible because only one user name can be seen from database logs. When same the web application server and database server of the same vendor is used and they have the ability, web application firewall and database firewall communicates correlates their logs between them. This provides the ability to map which database queries are executed to corresponding web application user. This is a very powerful integration that gives insight to the regarding people when things go wrong and investigation is needed.

Load balancers used in this part of the network to distribute the load to any number of servers. Also SSL offloading can be used to free CPU usage of the web servers. Load balancers also provide a flexible structure to add additional servers easily or stop problematic ones for fixing without downtime. No downtime maintenance is important for this organization considering the governmental services they maintain.

9.3.3 Vulnerability assessment and log correlation

There is a lot of security products are implemented so far but attacks mostly exploit known vulnerabilities on the systems to cause damage. Vulnerabilities should be remediated continuously along side with the other defending efforts. A Vulnerability scanner is added to the organization to automate the process of remediating vulnerabilities. This component scans the servers and clients periodically to find the vulnerabilities on them and a ticketing mechanism inside the system open tickets to asset owners for the found vulnerabilities on their system. This workflow is a cycle and makes the remediation processes a day to day work. Assuming the asset owners are working on their systems to remediate vulnerabilities, this system helps to keep clients and servers updated and free of known vulnerabilities.

Another issue is log correlation or in other words log management. Every device generates logs even if they are security devices or not. For the related personnel to investigate an issue or detecting a breach, it is very hard and inefficient for them to look to the logs of every different system. It is also possible to miss complex security incidents when someone is looking in to the log of a single device. To avoid this, log collection and correlation system is added to the network. It is also called as security information event management, SIEM for short. This device collects and stores logs from various devices and converts them to a single common format. Hence it is possible to correlate these logged events. For example consider an electronic card entry system is installed at the organization and every employee uses his or hers card to enter the building. The times when an employee enters and leaves are recorded to the log of system. SIEM system can collect the logs of this system and also login records from the directory server. A correlation rule can be written to search for a condition that the user is not in the building but he or she logged in to a system, which is a clear indication that the password is stolen or it is shared willingly. This is a simple example and for actual organizations there are no limits for the information that can be taken out by correlating and storing the logs in a common format.

Both of the systems are working like an ordinary server and has no topological effects so they are placed alongside with all other servers.

9.4 Local Area Network

As seen in Figure 9.4 most of the devices in the local area network are clients. Considering the precautions taken at the core level, there is only one network security devices in this segment and that is network access control (NAC) device. Host based products are very important when considering the security of the clients but they will be given in the proceeding chapters.

Client communications are inspected at the core network but to support all of this there is one step: preventing client systems that are not compliant with the policies to access the network. This is done via NAC device. NAC devices watches communication of clients such as the authentication process at directory servers or antivirus updates at a update server. Desired policies can be made to prevent client machines to access network, for example users that are not authenticated themselves with the directory services

NAC operates in two modes

- Pre-admission Control
- Post-admission Control

In preadmission control device inspects the client initially to grant access to network. If some client granted access for network and then their compliancy is not valid device prevents communication to the defined networks. After allowing a client to the network its behavior is inspected to detect malicious activity. For example after admission when a clients starts a port scan to determine ports on another device NAC can prevent its network operations and sends the client to a quarantine network service.

Two NAC systems are deployed because of the redundant structure, they are connected where the floor connections are made to the backbone to intercept at the first line when a client connects to network. Hence, NAC provides intelligent segmentation with controls can be done according to criteria such as checking directory login, antivirus updates, and installed products.

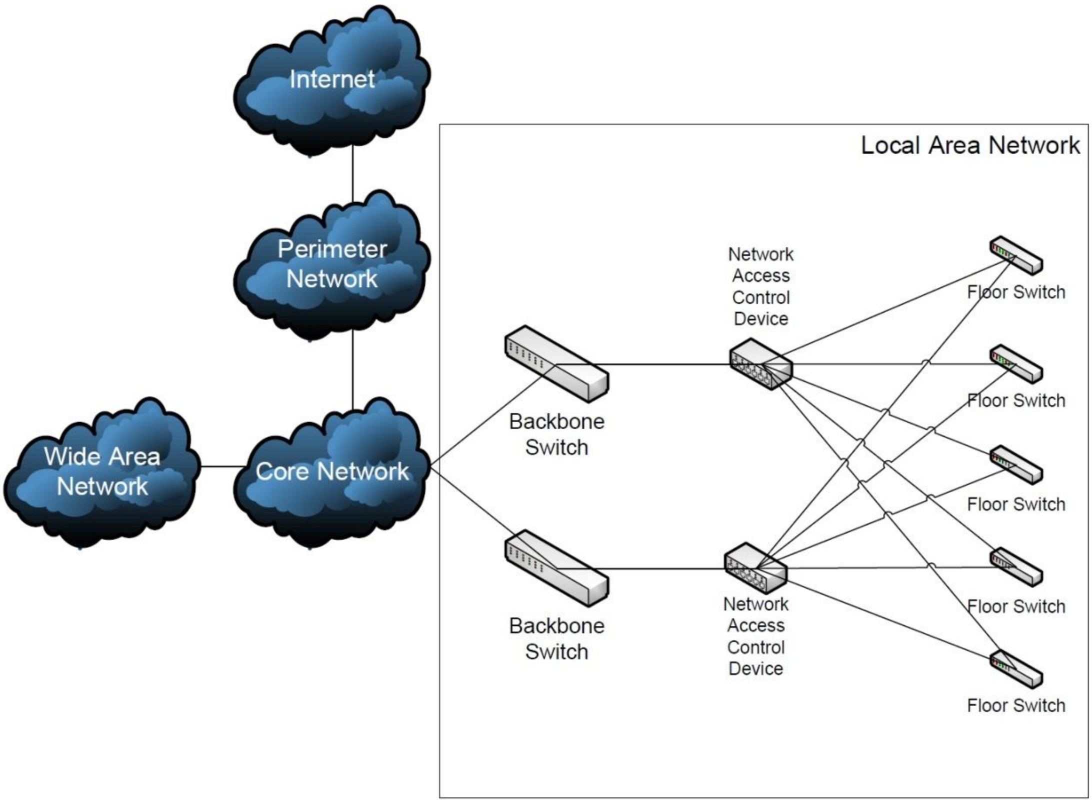


Figure 9.4 Details of the local area network

9.5 Wide Area Network

Wide area network includes the remote offices which have to connect to the organizational network through the internet. There are two examples in the Figure 9.5, one using a firewall/VPN device and the other is using a multipurpose protection device. The site using firewall device should have appropriate security products like the main organization network because no additional components are on simple firewall. Their connection is done with a virtual private networking (VPN) encrypted tunnel. VPN provides easy and secure connection through public networks. It is easy to use because existence of the vpn is not visible to the networks behind it. Private IP's are be used in both sides and there is no network configuration change required.

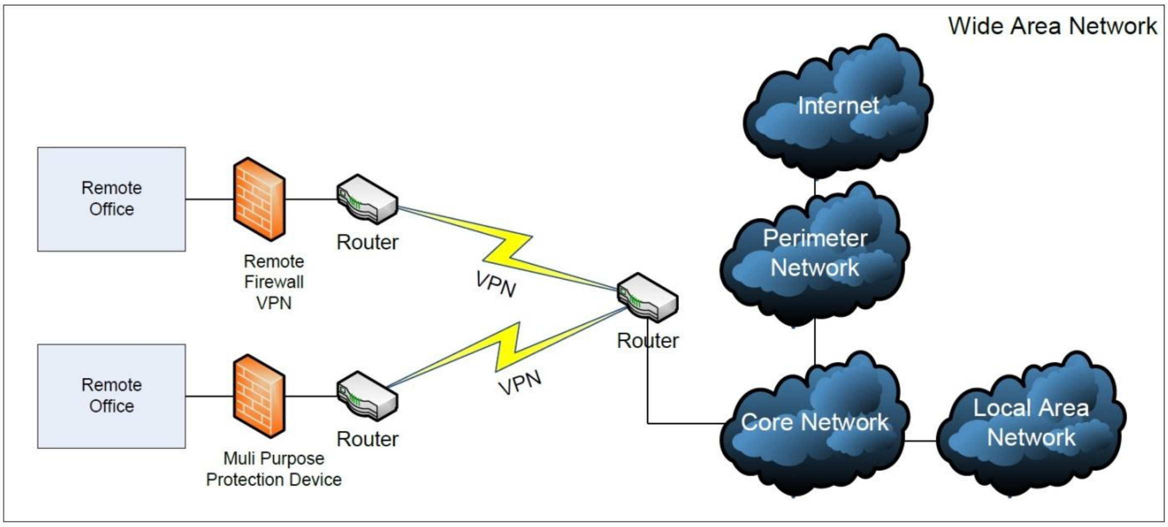


Figure 9.5 Details of the wide area network

The office with a multipurpose security device is relativity smaller than the other. There are 10 to 15 clients working. In order to apply security measure taken at core network multipurpose security devices are used which has built-in capability of more than one technology such as URL filter, antivirus, antispam, firewall, VPN, etc also commonly called as unified threat management (UTM) appliances. These type of offices connects to the central network with VPN same as the other more larger ones.

Regardless of the size and the firewall device used, every remote network connects directly to the core network segment.

9.6 Host Security Products

Host products are installed at the client workstations or server systems. Security software installed at the hosts is listed below:

- Antivirus
- Host Intrusion Prevention
- Host Firewall
- Host Data loss Prevention Agent
- Management Agent

All the components listed here are centrally managed by a management server. Management agent applies the configurations received from the server. Management agent is responsible for the installation and configuration of the components. By using central management in host products an improved visibility and control over clients are gained. Central configuration gives the power to administrators to apply a configuration organization wide. Hence, these host products act as a last line of defense against security threats except host DLP software. The aim of data loss prevention is, preventing unwanted flow from inside to outside rather than the other security issues which is mostly entering form outside to inside. Because of this fact host dlp is considered as the first line of defense for data leakages. By this mentality last line of defense is the network dlp at the core network. In order to assist this process, some vendors use device control features inside the dlp agent. Device control features provide the ability to prevent access to usb storage devices or cd/dvd burners. By this, data is prevented taken out by portable storage devices or other communications devices which are not permitted by the organization. Management of such products should be detailed to permit access for organization approved hardware or users that need access to such devices.

9.7 Evaluating the Architecture

As a result of this application, an architecture of security measures is given regarding the defined fictitious organization. Assessing the recommended architecture will be done in two parts. In the first part architecture will be discussed to make a decision that whether it is acceptable to the defense in depth mentality or not. In order to test this, defense layers for common threats will be evaluated. In the second part, functionality of the whole architectural elements will be mapped to the corresponding security controls.

9.7.1 Defense layers

In order to demonstrate that this architecture deploys more than one defense layer, following example threat sources are used:

- **Malware**
- **Vulnerability Exploiting**

Besides the given examples there are many threat sources can be added to these examples and also the given ones can be divided into more detailed items.

Malware:

There are several types of malware that target computer systems of an organization. Their purpose is also different from one another. In contrast, their detection and removal methods are similar by using security products. Delivering and executing the malicious code is required for a malware to infest a system. Therefore a malware can be stopped when it is propagating or can be stopped when it is reached to the desired system. For an effective malware protection malware scanners should be placed on the path to the system and also on the system itself. In Figure 9.6, arrows show the common sources of malware. URL filter, Antispam-Antivirus server and device control feature of dlp (data loss prevention) agent provide a preventive layer for malware propagation. This is done by preventing users to visit malicious sites and using portable storage devices that may be infected somewhere else. When these controls are not enough malware starts its travel across the network to reach the destination. Gateway antivirus scanner tries to determine malicious code on the traffic. This provides a protection on delivery phase of the malware. If gateway antivirus can’t detect the malware, it reaches to the target. As a last line of defense, antivirus product installed on the system deletes the malware if it is defined in the signature.

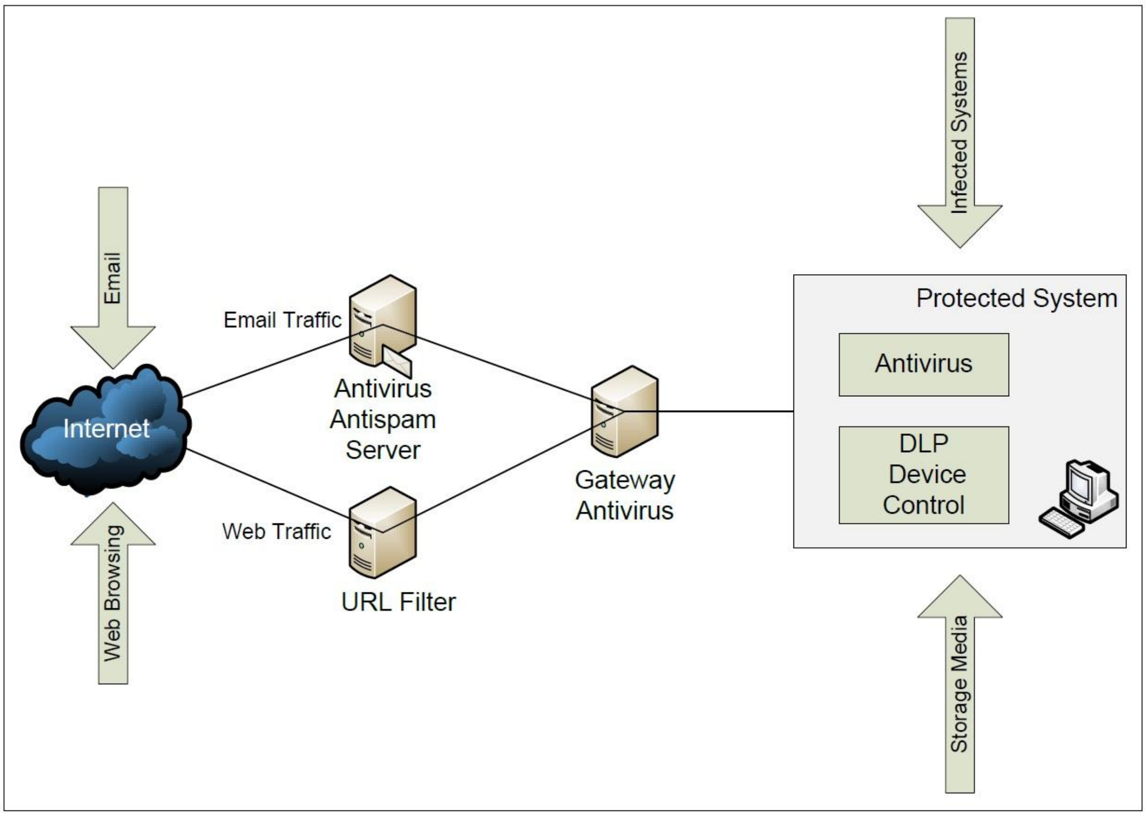


Figure 9.6 Malware defense

As a result, following stages constitute a defense in depth malware protection:

1. URL filter
2. Antispam-Antivirus
3. Gateway Antivirus
4. Host DLP and Device Control
5. Antivirus Software on the system

Vulnerability Exploiting and Availability:

Vulnerability exploiting, also called hacking, is using known vulnerabilities of a system to make it unusable, steal information or corrupt them for various motivations. Often vulnerabilities of the systems are fixed by the software vendor with updates. Most common example is operating system updates that fixes security related bugs. Hence it is very important that systems are running with the latest available patches to prevent hacking efforts. In order to exploit a vulnerability, there have to be an access to the relevant port between the attacker and the server. By closing the related ports on firewall is a preventive measure that prevents the attack even if the server is vulnerable or not. If all necessary ports are disabled attacker will probably attack from the ports that have to be open. At this point an IPS system is used to prevent attacks. IPS system scans the traffic to detect attacks like antivirus gateways detect a malware.

Usage of vulnerability scanner gives the ability to find exploitable vulnerabilities on the operating systems and applications. Even if it is not an active security device, vulnerability scanner acts as a preventive measure.

Load balancers are used to distribute the load to the servers. In addition, load balancer gives the flexibility of adding or removing servers from the load balancing pool that adds strength to availability of the system.

If the protected systems are web applications and databases, web application firewall and database firewall acts as a more sophisticated protection. As a last line of defense host based intrusion prevention software and host based firewall are used on the servers. This makes the IPS-firewall combination more resilient and accurate by reducing the configuration mistakes and increases the availability of IPS and firewall operations. According to Figure 9.7, when a web application is considered the layers of defenses are:

1. IPS
2. Firewall
3. Load Balancer
4. Web Application or Database Firewall
5. Host Based IPS
6. Host Based Firewall

If the considered server is not a web or a database server then layer 4 should be neglected. As a result of this protection layers, hacking to the servers are made much more difficult.

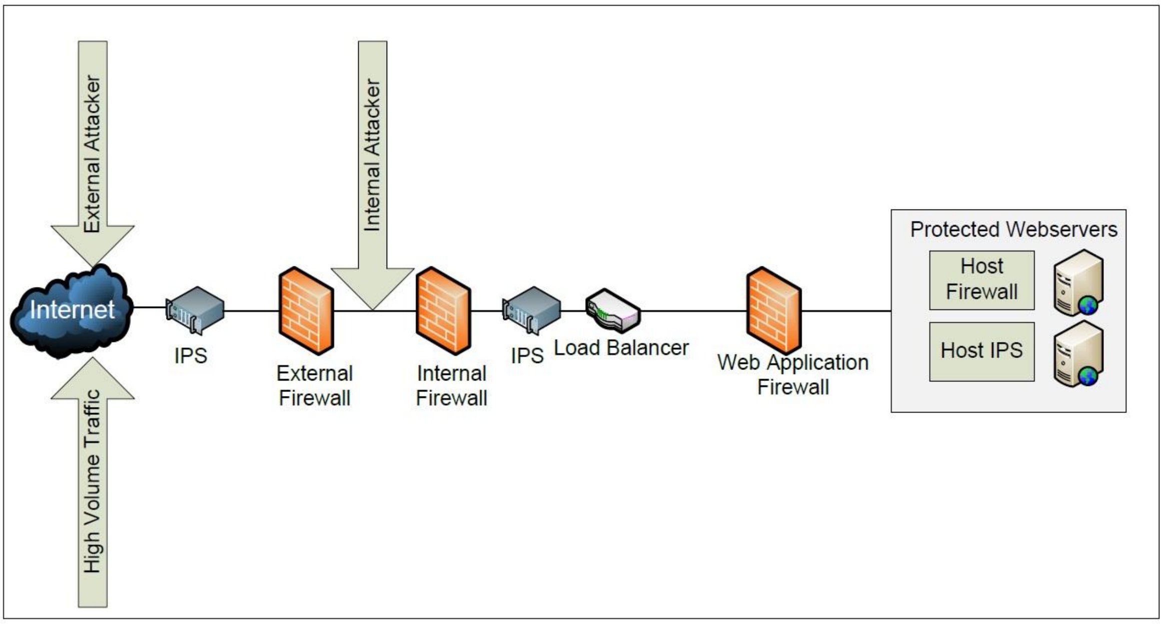


Figure 9.7 Defense of web servers

9.7.2 Security controls

It should be noted that the definition of information system term is more generalized in this thesis. Because of this, the previously mentioned recommended security controls of NIST are not directly compatible to this type of application. These controls are designed for software resources that organizations use to work with its data. Appropriate security controls are given in Table 9.1 with the relevant security device or system. Also some of the specific security controls are omitted in the list to show only controls that is related to the applied security elements.

Definitions of the security controls can be found in the related document of NIST but in Table 9.1 they are used as more general terms appropriate to the definition of IS in this study. Time stamps control can be given as example. In NIST standards it is defined as time stamping of the audit logs of the application used. In order to make a more generalized definition it can be defined as time stamping of the audit logs that are generated by all devices and application inside the information system. Other controls are evaluated by this method to match a corresponding security product.

Table 9.1 Security controls according to the used devices.

Security Control	Device
Denial of Service Protection	IPS
Boundary Protection	Firewall, IPS
Transmission Integrity	VPN
Transmission Confidentiality	VPN
Trusted Path	VPN
Cryptographic Key Establishment and Management	Firewall
User Identification and Authentication	Directory Service
Identifier Management	Directory Service
Audit Storage Capacity	SIEM
Response to Audit Processing Failures	SIEM
Audit Monitoring, Analysis, and Reporting	SIEM
Audit Reduction and Report Generation	SIEM
Time Stamps	SIEM
Protection of Audit Information	SIEM
Non-repudiation	SIEM
Audit Record Retention	SIEM
Account Management	Directory Service
Access Enforcement	Firewall, URL Filter
Information Flow Enforcement	DLP
Least Privilege	Directory Service , Firewall,
System Use Notification	URL Filter to show a message about use policy
Remote Access	Firewall

10. DISCUSSION OF RESULTS

As a result of this study a security architecture is developed by using common security products with defense in depth mentality. This structure consists of network security products and applications used on servers and clients. In later chapters it is mentioned that security is a wide field of study and when it is considered from technology point of view this kind of an application can be developed. But to say an organization is secure, there are additional parts that have to be considered. In order to simplify application development process, issues like organizational resources, management and people that are going to operate and use the systems are assumed to be handled correctly. In practical applications these parameters should all be investigated.

In the defined fictitious organization and in the result of the application all the configuration of devices and used software is assumed to be correctly configured. In a real world scenario this is hardly the case. Configurations of the devices that are used is important as themselves. For example a wrong configured firewall can easily pass traffic that is not wanted. Besides the configuration mistakes and deliberate configurations for illegal purposes are another concern. To prevent this in a real world application, defense in depth mentality should be applied to the configuration management process. Various confirmation levels should be placed for a configuration to be applied. Multiple people to confirm a configuration constitute a defense in depth approach to human factor of the issue. This ensures that applied configurations or changes to the system are not wrong and not against the organizations security policy. Monitoring changes in the configurations are also important to detect whether an officer bypassed this confirmation steps and apply any configuration.

Another issue is matching the real identity of a person to the correct digital identity of the user. As mentioned earlier authenticating a user’s identity can be done via something they have, something they alone know and something they are. Such methods can be applied with various technologies. Identification and authentication should be done in a way to eliminate the possibility of a person to impersonate another. Such an application maintains the basis of accountability.

Organization size and resources are also another concern of this type of application in real world. Proposed architecture is not directly applicable to many real organizations because the size and resources that are going to spend to security varies greatly. When size of an organization increases typically the infrastructure is become more and more complex. In order to deal with complex infrastructures custom designs should be developed to satisfy the security needs of the organization.

Human and other resources that an organization has, is another key factor in practical applications. A good balance should be made between spent resources and the value of the assets that are protected. Resources that are going to spend should not exceed the value of the assets.

Also an important issue is the security knowledge that management of the organization has. All managers in an organization should have a certain level of security awareness to make correct decisions when security related issues arise. Because they are decision makers, the success of an organization in security efforts are directly related to the security knowledge and awareness of the managers of any position.

11. SUMMARY AND CONCLUSIONS

11.1 Summary

In this thesis, information system security needs of an organization are presented and an application is developed to design a security architecture. Resulting architecture is offered as first step guide to the engineers who are going to restructure a network or deploy a security product mentioned here.

In the introduction chapter, the statement of the problem, related work, objectives and organization of the study is given. In order to introduce terminology information systems and related information is given. After this introduction, in chapter 3 security of information systems is discussed in general. Minimum security controls that are recommended by NIST are given in chapter 4 in order to establish a framework. Even if the controls are designed for a single application, some of them overlap with the security products that are mentioned in infrastructural security products.

Later, importance of risk analysis is discussed and risk assessment processes are investigated. Design considerations are given with the idea of defense in depth in chapter design for security.

A fictitious organization is defined for the application and it is assessed generally for security issues. Network infrastructure is changed to compartmentalize the network into groups surrounding the core network. In order to demonstrate the idea behind the architecture some threat sources are evaluated on the architecture.

11.2 Conclusions

Considering advancements in computer technologies, security of information systems is now a necessity for all types and sizes of organizations. Field of IS security is a vast subject and related to numerous types of technologies that are used today. Hence, the design and implementation of security features should be done with proper planning and risk analysis.

When organizations become larger, their dependencies to information systems increase proportionally. Such an issue makes complex and hard to manage networks. Security of such large information systems are also very hard to achieve and maintain. Because of this complex environment specialized products are more suitable to use.

There are custom applications that are developed by organizations. These applications are elevating the risk when security issues are not properly included into design. Therefore, when designing applications, security of the system should be added to the requirements. As for other aspects of an IS, infrastructural and host based security products are widely used. It is shown that some infrastructural security products close the gap caused by weak design or software bugs that may be present.

It is important not to depend to a single security product because of the threat complexity and motivation of today. Using the defense in depth mentality, designed security architecture will provide a layered approach to prevent attacks. Even if it is not directly applicable to all network structures, this architecture will give information and design tips to people who are working in this field.

An advantage of such architecture is the capabilities of multi layered defenses. Also according to the availability point of view redundant networking and other related devices provide more available services.

There are many types of security products used and their management can be a disadvantage of an organization which has low human resources. Another disadvantage is the available security budget and the management actions of the organization. This application recommends a lot of different type of software and hardware, because of this it will cost high amounts of money to buy the necessary devices and support services. There can be cases that the available budget is not enough or managers in the organization reluctant to spend necessary amount of money because of their lacking security knowledge and awareness. These kinds of obsticles are another side of organizations security efforts which is neglected in this application but have to be handled on actual organizations.

11.3 Extension of the Study

This study focuses on security field from a high point of view. Many attacks, specific security products and information technologies are not given in detail. More detailed and focused studies can be made on popular internet based technologies.

In an application like this study has, there will be always a sensitive information about security of organizations and this will make the applications difficult if not impossible for real organizations. A study that develops a network simulation framework for this issue can be supportive to all studies facing such confidentiality issues.

Also investigating new security product categories like traffic anomaly detectors or traffic capture devices will be useful. This kind of new technologies can close the gap between security issues and used traditional products.

LIST OF REFERENCES

[1] McAfee, Virtual Criminology Report 2009, 2009.

[2] Vacca, J., Computer and Information Security Handbook Morgan Kaufmann, 2009.

[3] Harrington, J., Network Security a Practical Approach, Elsevier, 2005.

[4] Wong, A. and Yeung, A., Network Infrastructure Security, Springer, 2009.

[5] Tipton, H.F. and Krause, M., Information Security Management Handbook, Auerbach, 2008.

[6] Lacey, D., Managing the Human Factor in Information Security, How to win over staff and influence business managers, John Wiley & Sons, 2009.

[7] Kanneganti, R. and Chodavarapu, P., SOA Security, Manning, 2008.

[8] Aktas, Z., Structured Analysis and Design of Information Systems, Prentice Hall International, 1987.

[9] O'Brien, J. and Marakas, G., Management Information Systems, McGraw-Hill,2008.

[10] Laudon, K. and Laudon, J., Management Information Systems: Managing the Digital Firm, Prentice Hall, 2007.

[11] Bentley, L. and Whitten, J., System Analysis and Design Methods, McGraw-Hill, 2007.

[12] Sommerville, I., Software Engineering, Addison-Wesley, 2007.

[13] Charles, K., Information Security Overview , Access: http://kellepcharles. blogspot.com /2008/01/information-security-overview.html, 2008.

[14] NIST, Recommended Security Controls for Federal Information Systems, 2007.

[15] NIST, Standards for Security Categorization of Federal Information and Information System, 2004.

[16] NIST, Risk Management Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technologies, 2002.

[17] Ye, N., Secure Computer and Network Systems, Wiley, 2008.

[18] Sosinsky, B., Networking Bible, Wiley Publishing, 2009.

[19] NIST, Guideline on Network Security Testing Recommendations of the National Institute of Standards and Technology, 2003.

[20] Ramachadran, J., Designing Security Architecture Solutions, John Wiley & Sons, 2002.

[21] Braude, E. and Berstein, M., Software Engineering: Modern Approaches, J. Wiley, 2011.

[22] Farah. G., Information Systems Security Architecture A Novel Approach to Layered Protection A Case Study, SANS Institute, 2004.

[23] Daswani, N. et al., Foundations of Security, Apress, 2007.

[24] NASA, Defense In Depth Access: http://www.nsa.gov/ia/_files/support/defenseindepth.pdf.