Technical report, IDE1012, February 2010

Network Security Issues, Tools for Testing Security in Computer Network and Development Solution for Improving Security in Computer Network

Master's Thesis in Computer Network Engineering

Amir Reza Fazely Hamedani, Sherin Skaria

School of Information Science, Computer and Electrical Engineering
Halmstad University

Network Security Issues, Tools for Testing Security in Computer Network and Development Solution for Improving Security in Computer Network

Master's thesis in Computer Network Engineering

School of Information Science, Computer and Electrical Engineering
Halmstad University
Box 823, S-301 18 Halmstad, Sweden

February 2010

Preface

This thesis report entitled "Network security issues: Tools for Testing Security in the Computer Network and development solution for improving security in the computer network" has been written for our Master Degree in Computer Network Engineering at Halmstad University, Sweden. This report includes a brief documentation of our research and also some parts of the implementation.

We would like to express our respect and sincere gratitude for our guides and supervisors, Professor Tony Larsson and Olga Torstensson, for all their motivation and their invaluable advice and devotion.

We also would like to extend our sincere appreciation to all those who have helped us in the completion of this project.

Amir Reza Fazely Hamedani & Sherin Skaria
Halmstad University, 12 February 2010

Abstract

This thesis tries to put forward a solution for improving the security of network. This study mainly focuses on information security standards, based on the ISO 27000 series.

Further, the thesis implements the suggested solution inside a simulated network and monitors and evaluates it by using the network vulnerability scanner.

With regard to the suggested solution, it is necessary to discuss the concepts of information security standards, and different security models and observe the advantages and limitations of them. Therefore, this research includes the definition of information security standards and the advantages and limitations of security models.

Contents

1 Introduction

1.1 Motivation

An increasing number of users, in addition to businesses in private network, demand access to Internet services such as the World Wide Web (WWW), electronic mail, Telnet, file transfer protocol (FTP) and so on. Security is of indispensable concern when an organization connects its private network to the Internet.

There will be upward apprehension about the network security of the organization for system administrators in the case of revealing private data and network infrastructure to the crackers and intruders in particular when those data should be transferred via network.

Every organization has to define a security policy to display the level of protection which they need to avoid unauthorized access to the resources of their internal network, and to defend against the unauthorized export of private information.

Even when connection to the internet is not established, it would be crucial to set up an internal security policy to control user access to part of the network and protect sensitive or classified information.

Information is considered as being an asset; it is vital to be accurately protected like other important business assets. This is particularly essential in the increasing business environments which are connected to each other as an effect of this growing interconnectivity.

Information is in numerous forms. It can be printed or written on paper, stored by specific electronic devices , shown on films, transferred via ordinary post or by electronic means or it can even be found in conversation.

Whatever forms the information takes, or by which it is shared or stored, it should always be thoroughly protected. In order to guarantee business permanence, minimize business risk, and maximize return on finances and opportunities, the security of the information and organization should be completely assured.

Information security is obtained by implementing a proper group of controls, including policies, processes, routines, organizational structures and software or hardware functions, which should be established, implemented, monitored, reviewed, and improved where required to guarantee the presence of particular security and business objectives.

1.2 Goals

This thesis aims to conduct a survey and practical experiments and provide solutions for the following issues:

- Understanding of security standard and discussing ISO 2700 series of standard
- Describing well known security models and analyzing the advantages and limitations of them
- Defining and analyzing well known network monitoring tools and discussing the advantages and limitations of each of them
- To discuss and provide a development solution for improving security of the network.

1.3 Methodology:

This thesis is in one part a survey that describes the effective method to improve security of the network with the help of some practical implementation.

The NESSUS and GFI LANGuard tools and Cisco's equipment have been used for implementation in our scenario.

1.4 Structure of the Document

Besides this introduction, chapter two covers the understanding of Information Security Standard and briefly defines different, well-known information security standards which are now in daily a day use in organizations, and briefly explains the basis of the one these standards that is directly related to information security.

Chapter three explains the concepts of security models and security policy and state machine models. Moreover, it gives the overview of different types of security policy based on confidentiality and integrity, and also offers some overview about their features and limitations compared to each other.

Chapter four addresses two network monitoring tools, Nessus and GFI LANguard, which are used to collect necessary information about the network environment by testing the specific network services and trying to show the existence of different computer services, including potential security vulnerabilities.

Chapter five tries to present how the security of the network is improved by mplementing the ISO 2007 router security checklist inside a sample network, and evaluates the security of the network by using a well-known network security scanner, called GFI LANguard, and analyzes the results which are obtained with by this tool.

The report ends with a conclusion about the results of this master thesis and presents a sample of a network security checklist based on ISO 27001 as an appendix.

2 Information Security Standards

2.1 Introduction

Nowadays, a huge range of security threats, from equipment malfunction to human errors, fraud, theft, damage, in so many countries, threaten organizations so that the need to protect information arises.

Information security indicates the need for protecting information from unauthorized access, use, exposure, interruption and alteration. The word "standard" is used inside the context of information security policies to distinguish between policies, standards and procedures.

To make the environment of an organization secure, all three levels of documentation should be preserved. The foremost goal of all information security standards is to focus on three main principles to guarantee information security, which are integrity, confidentiality and availability (Figure 2.1).

Integrity refers to the need to protect the unity and accuracy of the information as well as the methods used to process it. Confidentially refers to the guarantee that the information can only be accesses by the persons who have been permitted to utilize the information and all associated resources when needed. Availability refers to the guarantee that authorized users have access to information whenever they need it. [8]

Confidentiality	Guarantee that access to information is properly authorized.
Integrity	Safeguarding the correctness and unity of informational and processing methods.
Availability	Guarantee that authorized users have access to information when they need it.

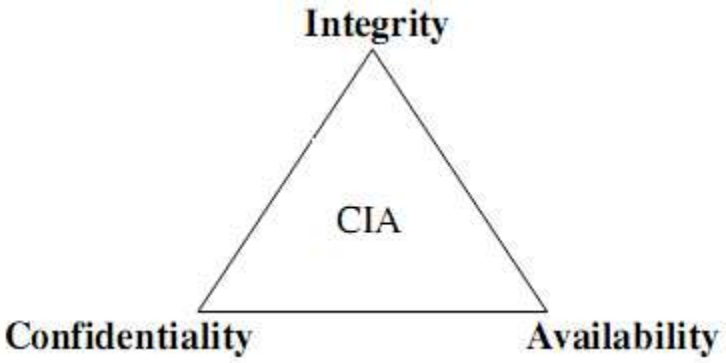


Fig 2.1 Security Cornerstones and definition of them

To manage information security and achieve the three major concepts of security in organization, one solution is to implement ISMS (Information Security Management System) and use the ISO (International Organization for Standardization) standards as a guide to increase effectiveness of ISMS; [2]
For example, to recognize information security risks in the organization, the organization may need to do a risk assessment. The best way to correctly evaluate the information is to think about

official requirements, in addition, to decide what its own requirements are to develop or improve your own information security program. BS17799 simply tries to help those who want to improve their information security requirement for overall safety.

From another point of view, because the information has value and is therefore an asset, it needs to be protected just like any other assets. Information should be protected just like the infrastructure that supports this information, including all the networks, systems and functions that enable an organization to control and manage its information assets. BS7799 explains the ways to protect organization's information assets. [1]

2.2 History of ISO Information Security Standards

The U.K Department of Trade and Industry (DTI) arranged a working group to work on codes for high-quality security practice, and the user version of this was published in 1989.

This standard was basically a list of security controls in which the practices were considerably suitable, normal, and as well as appropriate to the technology and environment of that era. The DTI code of practice for users was published as a British Standard (BS) instruction and, afterwards, was released as a BS with the name; BS 7799:1995 Part 1.Part 1 contains a list of controls of best practices for information security. [1]

A further part of the standard was introduced as BS 7799:1998, Part 2. The purpose was to provide a tool to assess and monitor Part 1, and to suggest a benchmark for certification. Following as the result of revision, Part 1 was published as BS 7799:1999, Part 1, was considered as an international standard (ISO), and published as ISO 17799:2000. Revision of Part 2 was published as BS 7799:2002, Part 2.

The standard ISO 17799 was once more edited and published as ISO 17799: 2005, then there was a name change, to ISO 27002:2005. In July 2007, BS 7799, Part 2 was submitted as an international standard and was released as ISO 27001:2005.Figure 2.2 shows the progress of ISO 27001 and the ISO 17799(ISO 27002). [2]

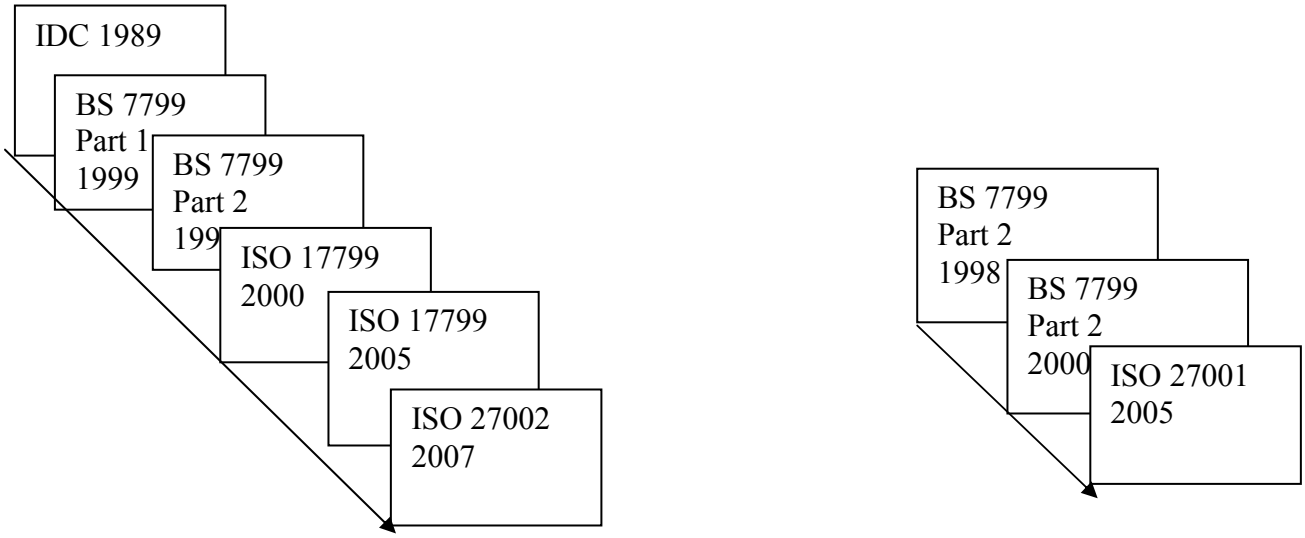


Fig 2.2 Developments of the ISO 27001 and ISO 27002 Standards

2.3 International Security Management Standards

Table 2-1 presents a list, and short explanation of some security standards that are, or will be, published in the ISO 27000 series. Anything marked "pending" is theoretical at the time of the writing of this report.

ISO/IEC	standard description
	(pending) vocabulary and definitions.
27001	information security management system requirements (specification)
27002	code of practice for information security management
27003	(pending) implementation guidance
27004	(pending) metric and measurement
27005	(pending) risk management

Table 2-1 (Taken from [2])

Organizations having been certified aligned with BS 7799, Part 2, should renovate their certification with the latest ISO 27001 standard. ISO 27002 is the new name for ISO 17799, ISO/IEC 27003 covers implementation guidance, and is based on BS 7799, Part 2; the date of publication of this standard is pending (at the time of writing this report).[4]

In BS 7799, Part 2 (and ISO 27001), the PDCA model (plan, do, check, act – is a scientific method to continuous improvement) is also covered and is used not only to enforce information security standards, but is generally used to enforce other management standards, including ISO 9001 and ISO 14001. ISO 27004 will focus on how to employ metric to measure the performance and efficiency of ISMS operations; once more, the publishing date is pending (at the time of writing this report). [2]

ISO 27005 will probably include risk management and will be similar to BS 7799, Part 3, which is about instruction for information security management. Additional organized standards at this time in the ISO 27000 series are ISO 27006, which is probably, contains the instruction for the certification or registration routine, and the ISO 27007 instruction for auditing information security management system. [1]

The standards are updated at least every two years in order to: [3]

- Provide a solution to the need of international organizations
- Develop best practices for information security
- Indicate to the lately deliberation in information security
- Stay aligned with other information security-related standards, such as ISO 27002(17799), COBIT v4.1 and PCI/DSS
- Include information on the latest 'hot topics'

2.4 The Necessity of Information Security

Information is now accepted as being a critical asset for most of the organizations and businesses in the world. The purpose of information security is the protection of organizational assets (in other words, information) from exposure by unauthorized or accidental modification, and guarantees that the information is ready for use when needed.

Conventionally, organizational asset space mostly consists of physical assets, like equipment and buildings, and negotiable ones, like stocks, bonds, currency or gold.

Thus, to remain viable, the organization must take information security seriously and implement effective ISMS, using a disciplined approach, for instance, ISO standards, as a guideline. ISO 27001 is designed to support this mission. It is easy to understand the results for an organization if its information is lost, damaged, corrupted, burnt, flooded, maliciously destroyed or abused. [3]

2.5 Introduction to ISO 27001 Standards

The ISO 27000 series of standards have been specially reserved by ISO for information security material. There is also a number of other topics, including ISO 9000(quality management), and ISO 14000(Environmental management).

The 27000 series will be populated with a range of individual standards and documents. Some of these standards (like ISO 27001) are already familiar, and have been published. Others are planned for publication, with final details about numbering and publication still to be decided. [5]

ISO 27002, Code of Practice, is usually used as an international standard for security of information in the world, and delivers various security controls to protect information and information technology.

The procedures introduced by this standard are actually useful in implementing the security controls in an organization and will show a discrepancy, according to the physical and technical environment.

ISO 27001 explains the requirement for an Information Security Management System (ISMS). It was built from BS7799 Part 2:2002. The range of any ISMS contains people, processes, IT systems and policies. It is not only appropriate for information held on computers, but also for all sections of industry and commerce. It covers all aspects and forms of information security. [2]

The information can be printed or written on paper, stored electronically, transmitted by post or email, shown on films, or spoken in conversation or any kind of form the information takes, or by which it is shared or stored**;** ISO 27001 will help an organization to be sure that its information constantly well protected. [1]

The ISO 27001 provides an ordinary model for implementing and operating ISMS, monitoring and improving ISMS operation, as well as obtaining a third-party international certificate to demonstrate that the security control exists and operates according to the requirements of the standard.

The ISMS should cover all parts of the organizational structure, planning activities, policies, routines, tasks, processes, practice and assets. ISO 27001 contains a number of controls which contain the following:

Security policy: The goal of this section is to offer management direction and support for information security.

Organization security: The goals of this part are:

- To manage information security inside the company.
- To take care of the security of information processing resources and organization information while being accessed by third parties.
- To take care of the security of information, whereas another organization has the responsibility for the processing of information.

Asset classification and control: The goals of this section are to keep suitable protection of corporate assets and to guarantee that information assets have the appropriate level of protection.

Personnel security: The goals of this section are:

- To decrease risks of human error, cheating, robbery or misuse of facilities;
- To guarantee that users are sensitive about information security threats and effects, and are prepared to maintain the corporate security policies in their normal work;
- To reduce the harm of security incidents or malfunctions and to recognize them.

Physical and environmental security: The goals of this section are:

- To avoid unauthorized access, harm and interference to business area and information;
- To avoid loss, harm or compromise of resources and disruption to business activities;
- To avoid compromise or theft of information and information processing facilities.

Communications and operations management: The goals of this section are:

- To guarantee the accuracy and protection of information processing assets;
- To decrease the possibility of the system failures;
- To protect the integrity of software and information;
- To keep the integrity and availability of information processing and communication;
- To guarantee the protection of information in networks and the supporting infrastructure;
- To avoid harm and interruptions to resources and business activities;
- To prevent destruction, modification or exploitation of information that is exchanged between organizations.

System access control: The goals of this section are:

- To control access to information;
- To prevent unauthorized access to information systems;
- To guarantee the protection of networked services;
- To avoid unauthorized access to computers;
- To identify unauthorized activities;
- To guarantee security of information when using mobile computing and tele-networking services.

System development and maintenance: The goals of this part are:

- To guarantee that the security is built into operational systems;
- To prevent destruction, change or misuse of user data in application systems;
- To protect the validity, integrity and confidentiality, of information;
- To guarantee that a protected way is used for IT projects and their support activities;
- To keep the security of application system software and data.

Business continuity management: The purposes of this section are to act against disruption to business activities and to protect business routines from the effects of major failures or disasters. [2]

2.6 ISO 27001 Implementation

To implement the ISO 27001 in order to improve the information security management system ISMS), three steps should be followed:

First, the objectives and aims of information security should be recognized and suitable policies have to be defined to achieve them. The result of this step will be a management framework for information.

Second, the security requirements should be identified by evaluation of security risks; the result will lead the appropriate management action.

Third, at the moment that the security necessities have been recognized, controls have to be selected and implemented. The controls need to guarantee that risks will be reduced to an acceptable level and should cover the particular security objectives of the organization.

Controls can be in the form of policies, practices, procedures, organizational structures and software functions which form organization to organization they will differ. After these three steps have been accomplished, the outcome will be a checklist which can be used to evaluate the level of information security in any part of the organization. Appendix A shows a sample checklist to assess the security of a network device (a router) based on ISO 27001. [5]

3 Security Models

3.1 Introduction

As mentioned before, computer security rests on confidentiality, integrity, and availability. Security policy recognizes the threats and clarifies the requirements to provide a secure system. Security method detects and prevents attacks and enables recovery as well.

A security policy is a set of rules and practices prescribing how important information is managed, protected, and distributed, and also expresses the precise security level by defining which security methods are to be performed. [7]

This is an important part that has a major role in defining the design of the system. The security policy is a base for the specifications of a system and provides the baseline for evaluating a system. A system provides trust by executing the security policy and also deals with the relationship between subjects and objects. [8]

The policy must point out which subjects can access different objects, and what actions are acceptable and unacceptable. To provide a level of trust which is acceptable, a system must be on the architectural foundation that provides the ability to protect itself from unreliable processes, intentional or unplanned compromises, and attacks toward different layers of the system.

A majority of the trust rating needs a specific subset of subjects and objects, explicit domains, and the separation of resources so the activities performed on them can be verified and their access can be controlled. [7]

A trust of the system is defined by a set of criteria. When a system is checked against this set of criteria, a rating is assigned to the system and is used by customers, vendors and the computing society. These criteria verify whether the security policy is being supported or implemented accurately. [8]

3.2 Security Models

Security model is a main concept in design and analysis of secure systems since it unifies the security policy that should be imposed in the system. A model is a symbolic demonstration of a policy by which the requirements of the policy makers would be mapped into a group of rules that should be followed by a computer system.

It is a conceptual term that represents the whole objectives and goals of a system which must be met and performed to be acknowledged as secure and acceptable. There are many complex steps during the system's design and development to make conceptual security policy feasible in the system.

A security model indicates the conceptual goals to implement the security policy in an information system by indicating necessary precise data structures and methods of performance. A security model is generally represented in analytical and mathematics facts, which are then mapped to system situations and, as a result, program developers will develop it through programming code. [9]

Hence, a policy is what encloses security goals like "each subject must be authorized to access each object". The security model takes the necessity and provides the essential mathematical formulas, relationships, and structure which should be followed to perform this goal. Specifications are developed from here for different operating systems (UNIX, Windows, or Macintosh), and single vendors can decide how to implement mechanisms that cover these necessary specifications.

As a basic example, if a security policy conveys that subjects to access objects need to be authorized, the security model would suggest the mathematical relationships and formulas describing how x can access y just through outlined specific methods.

Specifications are then developed to provide a link to what is in a computing environment and how it maps to components and mechanisms that are to be coded and developed. The developers then write the program code to create the mechanisms that provide a method for a system to use access control lists and give administrators some levels of control.

This mechanism provides a GUI representation for the network administrator, like check boxes, to choose what subjects can access what objects, and the possibility to put this configuration within the operating system. This elementary example is useful in presenting the relationship between the security policy and the security model**;** in reality, security models can be very complex. [6]

Some security models implement rules to guarantee confidentiality, such as the Bell-LaPadula model, while others implement rules to guarantee integrity, such as the Biba model. The above mentioned formal security models are used to offer high guarantees of security. Informal models, such as Clark-Wilson, are used more as a framework to describe how security policies have to be stated and executed.

A security policy indicates main goals with no idea of how they would be performed. A model is a framework that provides form to the policy and tries to find solutions for security problems for particular situations. Several security models have been developed to enforce security policies.

In other words, the security policy provides the conceptual goals, and the security model provides necessary things which should be done to accomplish these goals.

3.3 Security Policy

A security policy is a declaration of what is authorized, and what is not, while a security method is a process, tool, or procedure, for enforcing a security policy. A security policy defines "secure" for a system, or a set of systems, considering all relevant aspects of confidentiality, integrity and availability, and can also be informal or highly mathematical in nature. [9]

Concerning confidentiality, a security policy identifies those states in which information can be accessed by those who are not authorized to access it. Also, the policy must handle dynamic changes of authorization, so it includes a temporary element.

For example, a contractor working for a company may be authorized to access specific information for the duration of an agreement, but when that agreement expires, the contractor can

no longer access that information. This feature of the security policy is frequently called the *confidentiality policy*.

Concerning integrity, a security policy recognizes authorized ways in which information may be changed and identifies the entities which are authorized to modify it.

Authorization may be obtained from a variety of relationships, and external impacts may constrain it; for example, a rule called *separation of duties* prevents an entity from completing the transaction on its own, in many transactions. Those parts of the security policy that describe the situation and method in which data can be changed are called the *integrity policy*.[6]

Concerning availability, a security policy explains what services must be provided. It may present parameters within which the services will be accessible. For example, a browser may download Web pages but not Java applets. It may need a level of service by which a server will provide authentication data within a minute of the request being made. [9]

Security policies are often implicit rather than explicit. This causes confusion, especially when the policy is defined in terms of the mechanisms. For example, it will lead to confusion if some mechanisms avoid a particular action and others allow it and**,** therefore**,** the sites should avoid it.

As an example, the UNIX operating system was initially developed for a small research group. Therefore, it had appropriate methods to prevent users from damaging another's files accidentally.

The security policy, which is implied for this environment, was "do not delete or corrupt another's files, and any file not protected can be read". When the UNIX operating system moved into academic institutions and commercial and government environments, the previous security policy became insufficient; for example, some files had to be protected against individual users**'** access (rather than from groups of users). [8]

There are different models for confidentiality, integrity, and availability. Actually, none of them are fully trustworthy. The oldest of these models is the Bell/LaPadula model. A good integrity model of the time is Biba.

3.4 State Machine Model

In state machine models, the state is used to confirm the security of a system, which means all existing permissions and all existing instances of subjects which are accessing objects must be captured. Maintaining the state of a system is related to a subject's relationship with objects. [9]

When the subjects and objects are agreeing with the security policy then the subjects can have access to the objects. This system is secure.

State machines have provided a foundation for important security models. A state of a system is a snapshot of a system in one moment of time. There are many activities that can modify this state, which is referred to as a "state transition". [6]

Analyzing the security of a system necessitates an understanding of the mechanisms that enforce the security policy as well as knowledge of the related assumption and trust, which leads to the threats. Such knowledge allows one to design better mechanisms and policies to reduce the effects of threats. [9]

3.5 Types of Security Policy

Each organization has its own requests for the levels of confidentiality, integrity, and availability which are defined by that organization's security policy.

A military security policy (also called a governmental security policy) is a security policy developed mainly to preserve confidentiality while a commercial security policy is a security policy developed mainly to preserve integrity. The name comes from the need of commercial environments to avoid interfering with their data. [6]

3.5.1 Confidentiality Policy

Confidentiality policies emphasize the protection of confidentiality. The importance of these policies lies in what they provide, and their roles in the development of the concept of security. A confidentiality policy, also called an **"**information flow policy**"**, avoids the unauthorized exposure of information.

3.5.1.1 The Bell-LaPadula Security Model

Security models play an important role in providing concepts in the design and analysis of secure systems. They capture the security policy that should be enforced in the system. In the 1970s, the U.S. military used time-sharing mainframe systems and was concerned about the security of these systems and access to classified information.

BLP is used for implementing access control in military and government application. It was developed by David Elliot Bell and Leonard J. LaPadula, following the strong guidance from Roger R. Schell to formalize the U.S. Department of Defence (DoD). [7]

It was the first mathematical form of a multilevel security policy which is used to describe the ideas of a secure state machine, types and regulations of access.

The U.S. government had financed the development of this model to provide a framework for computer systems that might be used to store and process sensitive information.

The principal objective of the model is to avoid secret information being accessed in an unauthorized way.

A system that uses the Bell-LaPadula model is referred as a "multilevel security system" for the reason that users with different clearances use the system, and the systems process data with various classifications. [6]

The level at which information is classified determines the handling procedures that should be used. A subject that has top secret clearance can access top-secret, secret, and unclassified data. Top secret is the upper bound and unclassified is the lower bound.

The model utilizes subjects, objects, access procedures (read, write, and read/write), and levels of security; subjects and objects should be able to exist within different security levels and have connections and rules dictating the acceptable activities between them.

If accurately implemented and enforced, this model has mathematically affirmed that it will prevent data from a higher security level from flowing to a lower security level. It is also an information flow security model, in other words**,** information does not flow in an unsafe way. [7]

There are three principal rules used and implemented in Bell-LaPadula model: the simple security rule, the *-property rule, and the strong stat property rule.

The simple security rule expresses that a subject at a particular security level is not able to read data that exists at a higher security level. The *-property rule expresses that a subject in a particular security level is not able to write information to a lower security level.

The simple security rule is called “no read up” rule, and the *-property rule is called “no write down” rule. As shown in the Figure 5, the third rule, which is called the “strong star property rule”, expresses that a subject that has read and write abilities can just carry out those functions at the same security level, not anything higher**,** and not anything lower. These three rules show what states that the system can go into. [6]

The Bell-LaPadula model (BLP) is probably the most famous of the security models. It was developed by Bell and LaPadula at the time of the first concerted efforts to design secure multi-user operating systems. In this formal model, the entities in an information system are divided into subjects and objects.

This model is created based on the concept of a state machine with a set of permitted states in a computer network system. A system state is clarified to be “secure” if the only permitted access modes of subjects are in agreement with a security policy.

To find out if a particular access mode is permitted, the clearance of a subject is compared to classification of the object.

The Bell-LaPadula Model corresponds to military-style classification. It has persuaded the development of many other models and, indeed, much of the development of computer security technologies. [7]

This simplest type of confidentiality classification is a set of security clearances ordered in a linear arrangement (see Figure 3.1). These clearances correspond to level of sensitivity. The more sensitive information will be considered on the higher the security clearance (and the higher requirement to keep it confidential). [9]

The purpose of the Bell-LaPadula security model is to avoid the subject with lower clearance than the object’s security classification having read access.

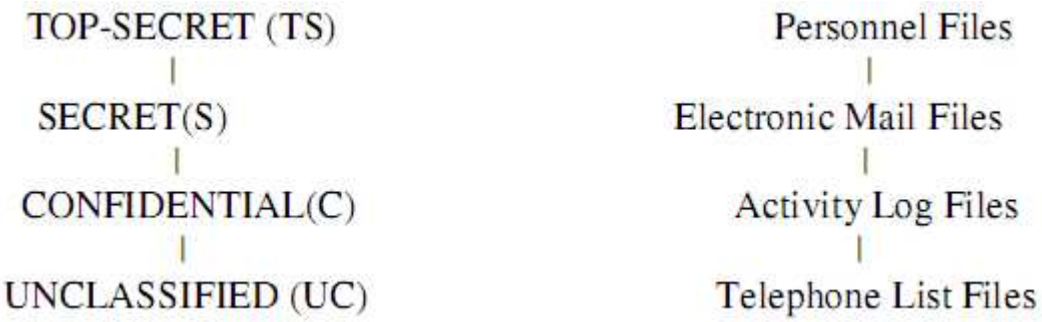


Fig 3.1 On the left is the basic confidentiality classification system. On the right is a set of documents grouped by their security levels.

Subjects and objects are assigned labels; the subject's label is a clearance label (top secret, secret, confidential, and so on) and the object's label is a classification label (top secret, secret, confidential, and so on).

When a subject attempts to access an object, the system compares the subject's clearance label and the object's classification label and searches the matrix to see if the activity is legal and secure. If so, the subject is given access to the object.

Now, if the subject's clearance label is top secret, and the object's classification label is secret, the subject is not able to write to this object, due to the *-property rule.

This verifies that subjects cannot unexpectedly or deliberately share confidential information by writing to an object at a lower security level (as Figure 3.2 shows).

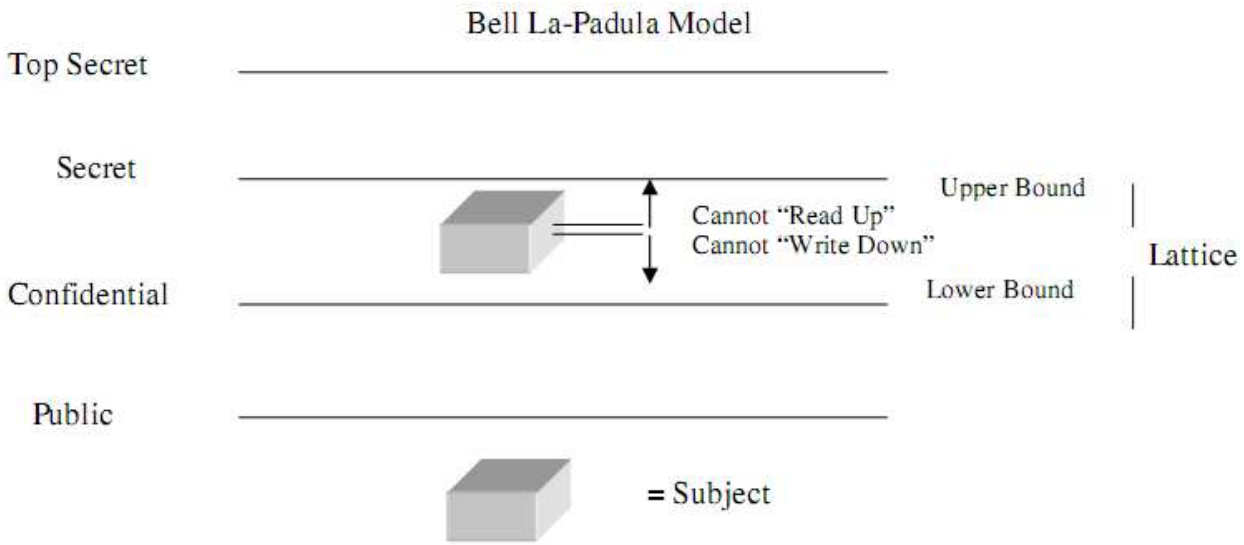


Fig 3.2 In the Bell-LaPadula model, each subject has a lattice of rights

An example of this kind of model is: The Data General B2 UNIX System.

The Bell-LaPadula Model affects all policy modelling in computer security. It was the first mathematical model to capture attributes of a real system in its rule. It formed the basis for several standards, including the Department of Defence's Trusted Computer System.

It is essential to state that this model was developed to verify that secrets remain secret; therefore, it refers to confidentiality only. This model does not refer to integrity of the data, in other words, it only states who can, and cannot, access the data. [6]

3.5.1.2 Aspects and Limitation of BLP

BLP is a very noteworthy security model: it has played an important role in the design of secure operating systems and**,** more or less**,** new models will be compared to BLP. The features of the BLP are as follows:

- The descriptive ability of the model: the set of BLP state represents all current access operations and all current access permissions.
- The security policies are based on security levels and an access control matrix. It is easy to introduce other structures in their place.

The fact the BLP defines security in terms of access control is a major reason for its popularity. Therefore, it is not too difficult to express the actions of an operating system or a database management system in terms of BLP. However, although it is an important security model, BLP does not cover all aspects of security. It has been criticised for dealing with confidentiality, not with integrity. [9]

As there is no mechanism to modify access rights, there is no management of access control through covert channels. (A covert channel is an information flow that is not under control by any security method).

The model does not consider file sharing, which is used in more modern systems. The absence of integrity policies is a feature of BLP, rather than a fault, as it is quite realistic for a security model to limit its goals. BLP has no policies for the modification of access rights. As a matter of fact, BLP was originally designed for systems where there is no change of security levels. [6]

Designing complex systems describable by complex models leads to difficulty in finding proof of security. In the worst case, a general algorithm that confirms security for all difficulties does not exist. To verify security properties, it is better to limit the complexity of the security model. Such a model may not describe all wanted security properties, but it is an efficient method for verifying "security".

On the other hand, it would be advisable to design simple systems that can be adequately described in the simple model. If there is too wide a gap between a system and the security model, proof of security in the model will be difficult.

3.5.2 Integrity Policies

Integrity policies focus on integrity rather than confidentiality, because most commercial and industrial environments are more worried about correctness than disclosure.

For example, in a commercial organization, an inventory control system may function correctly in case of releasing the data it manages; but it cannot function correctly if the data is accidentally changed. So integrity, rather than confidentiality, is a key in these kinds of firms.

Integrity models are increasing in variety and popularity. The importance of this model will continue to increase while more and more commercial environments develop models or policies**,** in order to assist them to protect their data. [9]

The goal of these kind of policies is commercial requirement, which is different from the military requirement, meaning that their emphasis is on keeping data integrity, as described below**.** Users will not write their own programs; they can use existing production programs and databases.

Programmers, by using a system which is not productive, develop and test programs. If they require access to real data through a particular process, the production data will give to them, but they should use it on their development system. To install and use a program from the development system onto the production system, a special procedure is followed. [6]

Auditors and managers should have the right to use both system state and system logs. These requests suggest several rules of operation:

Separation of duty:
The rule of separation of duty requires that, if two or more steps are required to perform a crucial function, at least two different people should perform them. Moving a program from the development system to the production system is an example of a critical function.

Separation of function:
Developers not only do not build up new programs on production systems due to the potential risks to production data, but also do not process production data on the development systems.

Depending on the sensitivity of the data, the developers and testers may receive cleaned production data. In addition, the development environment must be as similar as possible to the actual production environment.

Auditing:
Commercial systems stress on recovery and responsibility. Auditing is the process of analyzing systems to determine what actions occurred and who performed them. Hence, commercial systems should provide comprehensive auditing, and thus have extensive logging (the basis part for most auditing).

It is of considerable that the requirements of a commercial environment differ from a military environment. In a military environment, users require authorization to have access to particular categories. Therefore, security levels provides accessibility to information in those parts.

On the other hand, commercial companies rarely grant access based on “clearance”; if a particular user needs to have access to the specific information, he or she will be given it.

Although this can be modelled using the Bell-LaPadula Model, it requires a large number of categories and security levels, which increases the complexity of the modelling.

Difficulties arise in controlling the growth of categories and security levels, as well as handling information aggregation. Commercial firms usually allow a limited amount of harmless information to be published and keep a large amount of sensitive information confidential.

When the harmless information is aggregated, one can often figure out much sensitive information. To prevent this, a model to track what questions have been asked should be used**,** and this is extremely complicated. It should be mentioned that Bell-LaPadula Model does not have this ability. [7]

3.5.2.1 Biba Integrity Model

In 1977, Kenneth J. Biba introduced Biba Model, or Biba Integrity Model, which studies the nature of the integrity of systems. It was developed after the Bell-LaPadula model.

Biba utilizes a state machine model and closely looks like the Bell-LaPadula model. The difference between these two is the Biba Model considers the integrity of data.

In this model**,** data are in danger when subjects at lower integrity can write to objects at higher integrity levels and when subjects can read data at lower levels.

If Biba model implemented and applied correctly, it forbids data from any integrity level flowing to a higher integrity level. Subjects and data are grouped into organized levels of integrity. [6]

The model is designed in order that subjects may not damage data which is ranked in a level higher than the subject, or be damaged by data from a lower level than the subject. [7]

Biba has two principal rules in offering this type of protection. The first rule mentioned is the “no write up”, and it expresses that a subject is not authorized to write data to an object at a higher integrity level.
The second rule mentioned is the “no read down”, and it expresses that a subject is not authorized to read data from a lower integrity level. Although the second rule looks a little strange, it is protecting the subject and data at a higher integrity level from being corrupted by data in a lower integrity level.
In general, the protection of data integrity has these goals:

- To avoid authorized data change by unauthorized parties.
- To avoid unauthorized data change by authorized parties.

This security model is described by the expression: “no read down, no write up”. This is in comparison with the Bell-LaPadula model, which is described by the expression “no write down, no read up”. Like the Bell-LaPAdula model, the Biba model specifies a set of rules. These rules are the opposite of the Bell-LaPadula rules:

- The first rule, which is called "simple integrity rule", states that a subject at a particular level of integrity is not authorized to read an object at a lower level of integrity (no read down).
- The second rule, which is called "*(star) integrity rule" states that a subject at a particular level of integrity is not authorized to not write to any object at a higher integrity level (no write up)

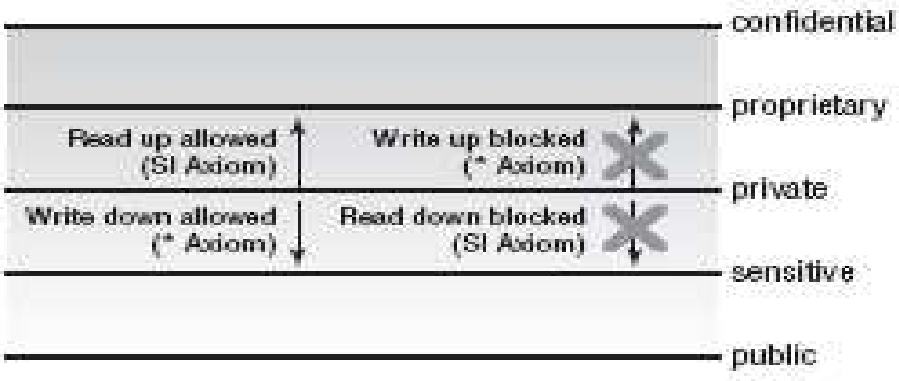


Fig 3.3 Biba Integrity Model [Taken form (6)]

The higher the level, the users will have more confidence that a program will execute correctly. Data at a higher level is more accurate and/or reliable than data at a lower level.

Once more, this model implicitly includes the concept "trust"; actually, the term "trustworthiness" is used as a measure of integrity level. As an example of implementation of this security model, Pozzo and Gray implemented Biba's integrity model on the distributed operating system LOCUS. Their goal was to limit execution domains for each program to prevent data from being altered by untrustworthy software. [9]

When somebody first learns about the Bell-LaPadula and Biba models, these two appear very similar, and the reason for their differences may bring some confusion. As mentioned, the Bell-LaPadula model was written for the U.S. government which is extremely worried about the outflow of their secret information.

In this model, a user is not authorized to write to a lower level because that user may let out some secret information. Similarly, a user at a lower level is not authorized to read anything at a higher level because that user may can access and learn some secrets. [6]

However, not everyone is so worried about confidentiality and only a few people have such important secrets to protect. The commercial industry is more worried about the integrity of its data. Accounts are more worried about keeping their numbers correct and making sure decimal points are not dropped, or extra zeroes added, during a process carried out by an application. [7]

The accounting companies would prefer to use the Biba model because they are more concerned about the integrity of this data, which is at little risk of being stolen by someone. Surely, in the

real world, the accounting company does not search for the name “Biba” on the back of a product to verify that it is in the design of their application.

This is something that was concluded and enforced when the application was being developed. The consumers use the security rating to decide if a system is suitable for them. Therefore, even though the auditors are using a system by means of the Biba model, they would not know. [6]

3.5.2.2 Clark-Wilson Integrity Model

David Clark and David Wilson developed an integrity model**,** which is totally different from previous models**,** in 1987. It was developed after Biba, and used some different approaches to protect the integrity of information by focusing on preventing authorized users from making unauthorized data modifications and cheating, and to avoid errors within commercial applications. [7]

The model was described in a paper named “*A Comparison of Commercial and Military Computer Security Policies*”. Information integrity is maintained by preventing corruption of data items in a system due to either error or malice.

In the Clark-Wilson model, users cannot access and use objects directly, but can access the object through a program. This provides another layer of protection between the subject and the object and further limits the type of actions that can take place on that object, so this will protect the integrity of the object.

The program has its own set of limitation which expresses what actions the users can**,** and cannot**,** perform on objects. This organizes the way objects are protected and reduces the methods that could cause the data to be corrupted or changed in an unwanted way.

This model also is based on *separation of duties*, which divides the operation into different parts**,** and different users or rules are required to perform each part. This guarantees that an important task cannot be performed by one entity. Auditing is also required in this model to keep track of the information coming from outside of the system.

The Clark-Wilson model prevents permitted users from making any changes to the data by forcing them to go through programs to modify objects, or by implementing separation of duties. [9]

3.5.3 Hybrid Policies

There are a few organizations which restrict their security goals only to confidentiality or integrity; most of them need both. Two very early such models are: The Chinese Wall model, which is extracted from the British laws regarding conflict of interest, and the second, is the Clinical Information Systems security model, which is extracted from medical ethics and laws about the spreading of patient data.

3.5.3.1 Chinese Wall Model (Brewer and Nash Model)

The Chinese wall model, designed by Brewer and Nash, was produced to grant access controls that are able to change dynamically, depending on the user’s earlier actions.

The main goal of the model is to prevent users from accessing data that could be seen as conflicts of interest. This model provides access rules in a business where analysts have to be assured that no conflicts of interest occur when they are dealing with different clients (companies).
These access controls can change dynamically, according to the user's behaviour and previous access requests. It is a security policy model that is equally related to confidentiality and integrity. The main ordinary environments for this model are stock exchanges or investment houses. [6]

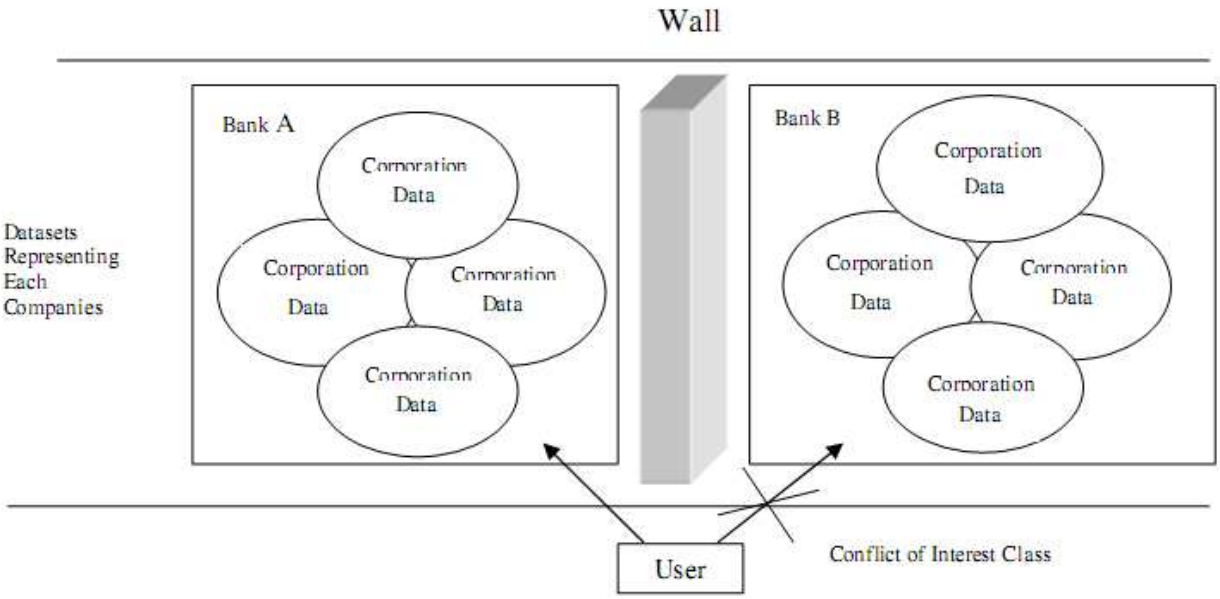


Fig 3.4 The Chinese Wall model provides dynamic access control.

3.5.3.2 Clinical Information Security Policy

Medical records need policies that merge both confidentiality and integrity. The critical problems are not conflicts of interest but are patient confidentiality, authentication of both records and staff who edit and update those records, and the guarantee that the records have not been changed incorrectly.
Anderson, who developed this model, remarks that the Bell-LaPadula security model is a subset of the Clinical Information System Security model. In point of fact, the Bell-LaPadula Model concentrates on the subjects accessing the objects, whereas the Clinical Information System Model concentrates on the objects being accessed by the subjects (since there are more patients, and medical records, than clinicians). [9]

4 Tools for Assessing the Security of the Network

4.1 Introduction

The network monitoring tools gather necessary information about all the computers and networks by testing the specific network services**,** such as finger, NFD, HTTP, FTP, SMTP and other services.

The information which is gathered shows the existence of different information services**,** including possible security vulnerabilities. These security vulnerabilities typically appear due to improperly setup or configured network services or equipment, the presence of notorious bugs in system utilities or weak policy implementation or design.
There are several network assessment and monitoring tools around to assess the security of the network but, according to the survey released by insecure company in 2006-7, which asked 3243 hackers to name their favourites tools, the favourite vulnerability scanner tools are: 1-Nessus, 2-GFI LANGuard, and 3-Retina. We use Nessus and GFI LANGuard in the lab to find out the security vulnerabilities which exist on the simulated network and understand how they work.

4.2 Nessus

Nessus is a powerful and simple to use free remote network security scanner. Nessus offers an environment to audit a given network remotely, and discover if there is some vulnerability inside the network which hackers can use to get into it, or mistreat it in some way.

Because every computer has thousands of communication paths, which are called ports, some services may listen to them for related communication packets. Nessus first recognizes what service is running on the ports by testing each port then, by testing the service, it tries to discover if there is vulnerability in that service which can be used by a hacker.

Nessus does not notice that a specific service is always running on a specific port. This feature is completely different compared to the other security scanners and it means that, for example, if a mail server is running on port 1111 for the security consideration, it will discover it and test if it is secure.

Another important feature this software has is that Nessus does not recognize that a particular service has vulnerability because of the version of that remote service; this means that it will actually try to exploit the vulnerability of the service.

Another powerful feature of the Nessus is that, by default, it can do more than 7000 security vulnerability tests, which are separated into 23 different categories, such as: different backdoors, CGI vulnerabilities, CISCO, DoS(denial of service), finger misuse, firewalls, FTP, earn root privilege remotely, Netware, …

By providing a scripting language, the administrator can write their own script to test a particular system; this feature makes the Nessus very extensible.

In addition, it must be mentioned that Nessus is a remote scanner, so it is not required to be installed on a computer to test it. This means that it can be installed on only one computer and test the all the computers on the network.

Nessus consists of two major parts: a server and a client. The role of server part is to run all the scans and the role of the client part is to control the scans and observe reports. The structure of the Nessus, which is based on client-server architecture, provides capability for the server, which acts as scanner, and the client, which acts as graphical user interface (GUI), to distribute in several configurations. This allows the use of one server by several clients, reducing management costs.

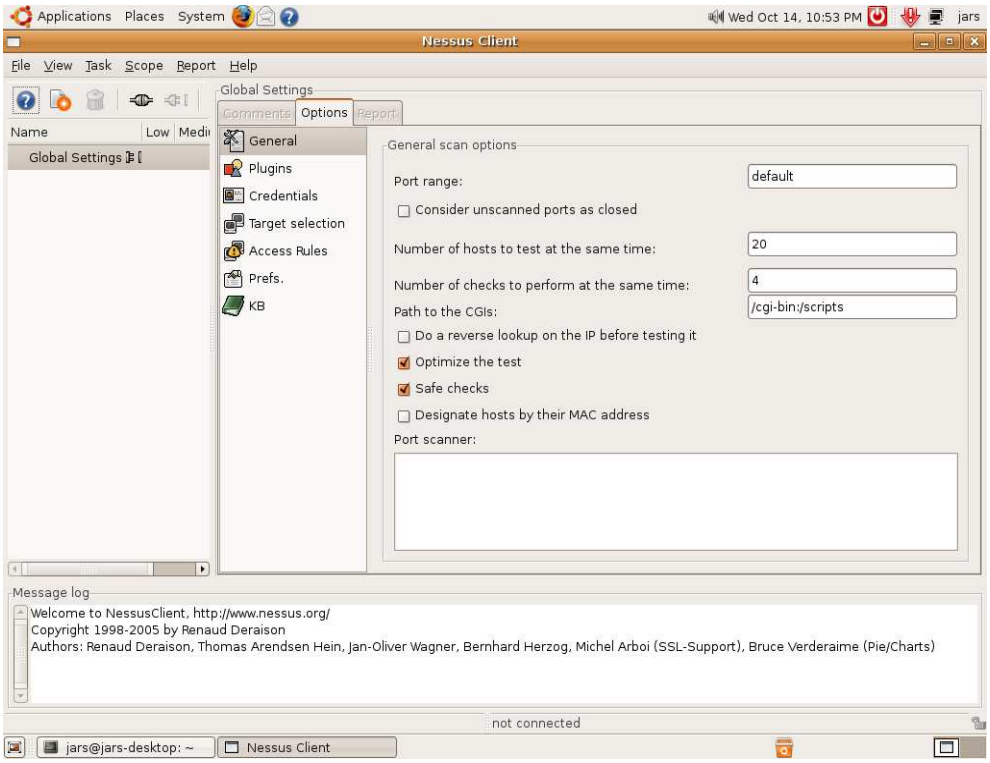


Fig 4.1 The main page of Nessus Client software

4.3 GFI LANguard

The GFI LANguard is a vulnerability scanner for the network which offers a centralized environment for the IT administrators of the organizations to discover and solve security vulnerabilities by scanning computers on the network.

This software is produced in two versions: one as a licensed product and the other as a free version. The free version of this software has all available features but a maximum of 5 IP addresses can be scanned**.** However, the licensed product can be used for larger networks with numerous IP addresses.

This is a powerful tool for scanning and auditing all the computer ports for the existence of known vulnerabilities and also for the security of the network.

One of the important features which makes this software more powerful is that it offers central patch management abilities, which provide a central environment for downloading and distribution of patches to systems which are recognized to have vulnerabilities. This means that this software has the ability to perform like both a patch manager and vulnerability scanner.

It has also some strong features**,** such as gathering all the network's important information, like network devices and identification of the device type**,** such aswired, wireless or virtual.

It recognizes wide range of vulnerabilities for different network services and open shares on the computers and lists the all users who have access to these shares and permissions these users have.

The above mentioned feature provides the ability for this software to act as a network audit.

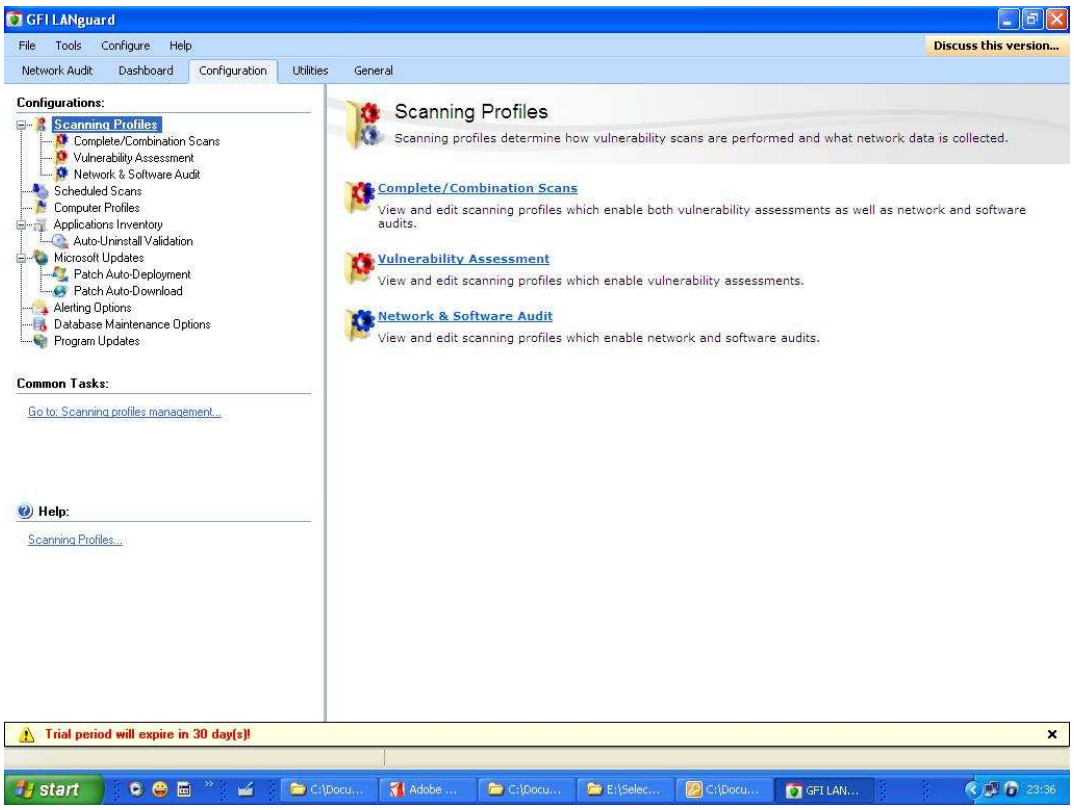


Fig 4.2 The main page of GFI LANguard Scanner

This software also has the ability to find**,** and alert about**,** unauthorized software which is installed on the computers of the network and can uninstall it automatically. One of the features which can be expressed as a weakness of this software is the report is not included inside of main software, and it mean another software program should be installed separately for generating the management report.

5 Implementation

We have carried out a simulation on the available equipment where we used the network, as shown in figure below. We have carried out the entire process of improving the security of network by using ISO 27001 standards and evaluating the result by using network vulnerability scanner tools.

To reach the above aim, we devised a scenario which simulates a real network by using two desktop computers, a router and a switch, and also using GFI LANguard software (introduced it in previous chapter) to evaluate the security of the network both before, and after, implementation of the security solution inside the network. (Figure 5.1)

Particular ISO 27001's controls, that consider the network entities have been used to create a sample checklist for implementing security for routers inside the network (Appendix A). After installing the network with the above mentioned entities, first, we evaluate the security of the router and overall network entities both, by using the Network vulnerability scanner. Then, we implemented the checklist on the router and again evaluated the same entities, and tried to establish how the security of the network had been affected and improved by using the checklist based on ISO 27001.

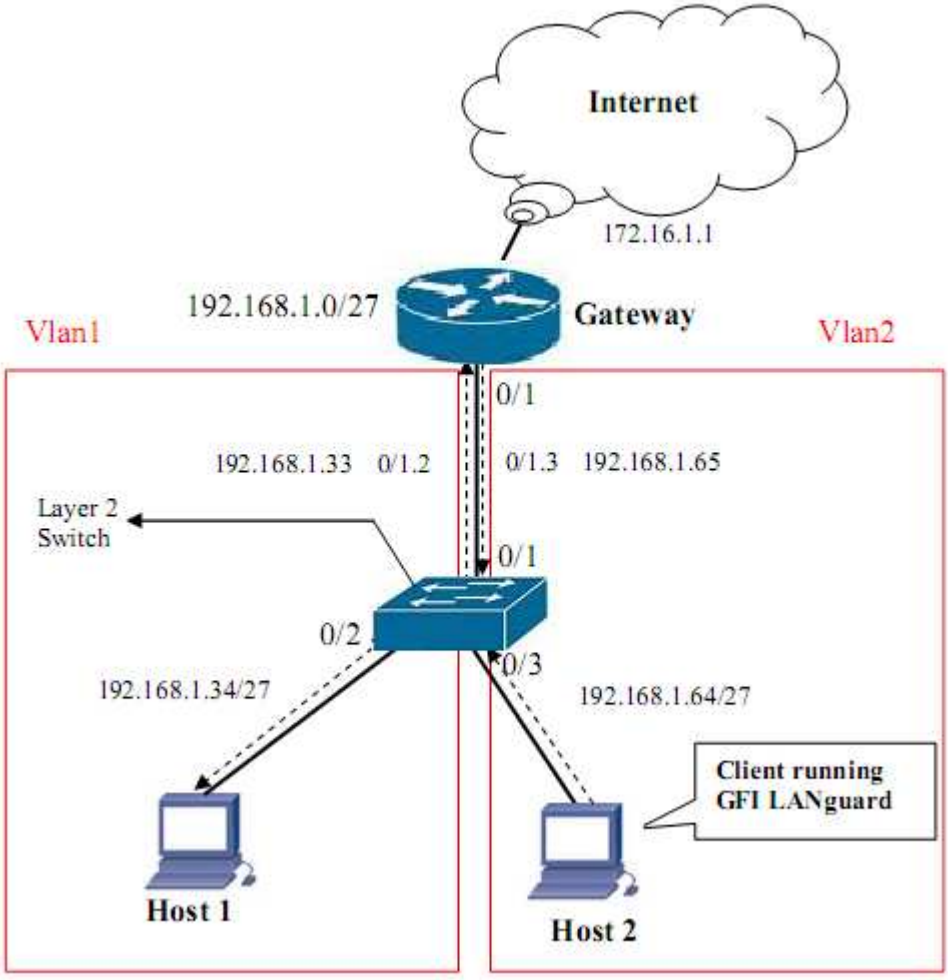


Fig 5.1 Structure of the sample network

5.1 Equipment

For implementation, we used Cisco's devices (one router, one switch) and two desktop computers, to simulate an actual network (Table 5.1).

For evaluating the result, we used the GFI LANguard tool, which is installed on one of the clients inside the network.

Devices	Description	Quantity
Router	2800 Series	1
Switch	2960 Series	1
Desktop Computer	Pentium V	2

Table 5.1 Equipments

5.2 Design of the Network

The network contained one router and one switch, with two other hosts, in order to make the simulation environment more similar to the real network; the hosts are separated in two different virtual LANs, i.e vlan2, vlan3

VLAN stands for "virtual local area network", and it extends beyond a single traditional LAN to a group of LAN segments, and given specific configuration. It provides improved administration efficiency, virtual groups, reduction of routing for broadcast containment and enhanced network security.

The router is configured to support two different networks as a router on stick. The trunk line is established between router and switch and the remaining switch ports are in access mode. The network which is designed is scalable and, in future, we can start increasing the support for extra network devices, according to the requirements.

By using *ping* command, it can be assured that all hosts in different networks can interact with each other. Host2 is equipped with all required hardware and software support for scanning a network. Here, we are mainly making use of GFI LANguard software.

5.3 Result

By evaluating results contained in the research papers and websites, and the results from practical work, we have concluded that the security level has improved significantly, i.e. by 50%.

GFI LANguard is a security scanning tool and it allows a network administrator quickly and easily to automate tracking which machines are vulnerable for deploying the patches, and also it creates the report which we can use to fix the security issues on a network.

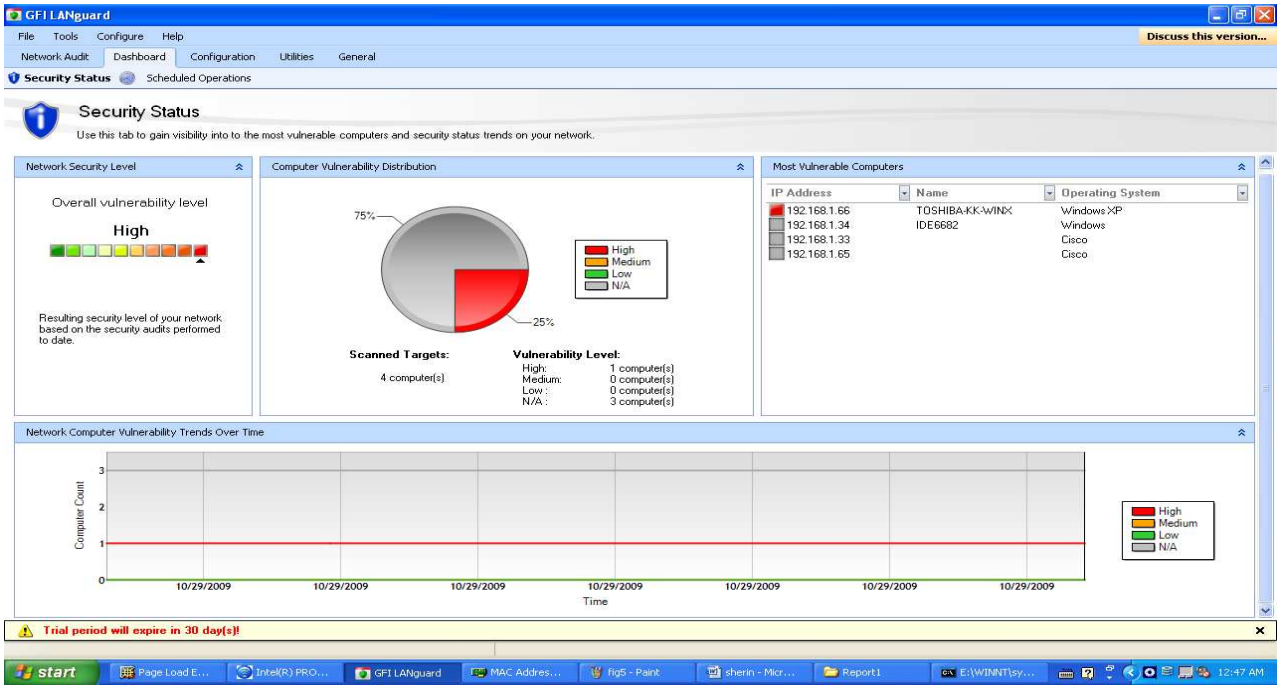


Fig 5.2 Security status before installing scanning tools

The Figure 5.2 presents the simulation result of the network that we built without configuring and implementing any security policy for the network entities. It should be considered that, in this network, out of four computing devices, one only device is completely secured, namely host2.

This particular device is secured because it is a personal computer, which has already some preinstalled security software, but actually it is not secured for the network activities.

Here, you can see that the network 192.168.1.66 is well secured, and the other three devices are not secured, which shows a very bad security level. It also means that this network is vulnerable for different internal/external attacks.

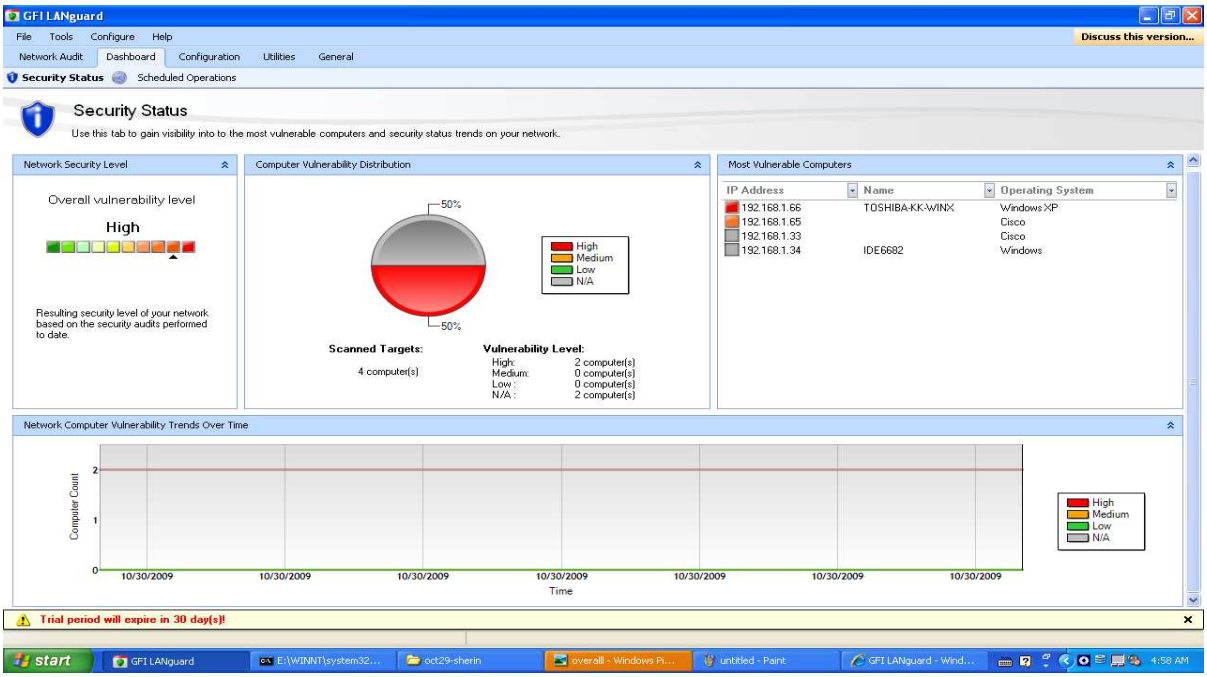


Fig 5.3 Security status after implementing security checklist

Figure 5.3 proves the higher security level compared to the previous diagram, this is because the simulation result was taken after implementing the ISO 27001 security check list.

The main process of GFI LANguard is to scan all the devices and network. At first, before implementing any security policy, the percentage of the network security was 25% by using GFI LANguard but, after implementing security policy, the security level increased to 50% from 25 %.

Consequently, as it scans the router for the known vulnerabilities and then protects against these vulnerabilities by using the ISO 2007 router checklist, the level of the network security increases and protects the network from the intruders. We can check that the network 192.168.1.66 belongs to the personal computer (host 2), and the network 192.168.1.65 belongs to the CISCO router is under the secured level.

Network Vulnerability Summary Report

Scan reference : 192.168.1.1-192.168.1.95
Scan date & time : 30-Oct-2009 3:46

Hosts Severity Level Distribution

Vuln. Severity	Vuln. Count	%
High	30	77
Medium	1	3
Low	8	21

Top 10 Vulnerable Hosts (by Severity)

IP Address	Host Name	Severity		
		High	Med.	Low
192.168.1.66	TOSHIBA-KK-WINX	30	1	3
192.168.1.65	N/A	0	0	2
192.168.1.33	N/A	0	0	2
192.168.1.34	IDE6682	0	0	1

Fig. 2.2

Fig. 2.2

Fig. 2.2

Fig 5.4 Network Vulnerability Summary Report before Configuring Security tool

Network Vulnerability Summary Report

Scan reference : 192.168.1.1-192.168.1.95
Scan date & time : 30-Oct-2009 2:34

Hosts Severity Level Distribution

Vuln. Severity	Vuln. Count	%
High	32	74
Medium	1	2
Low	10	23

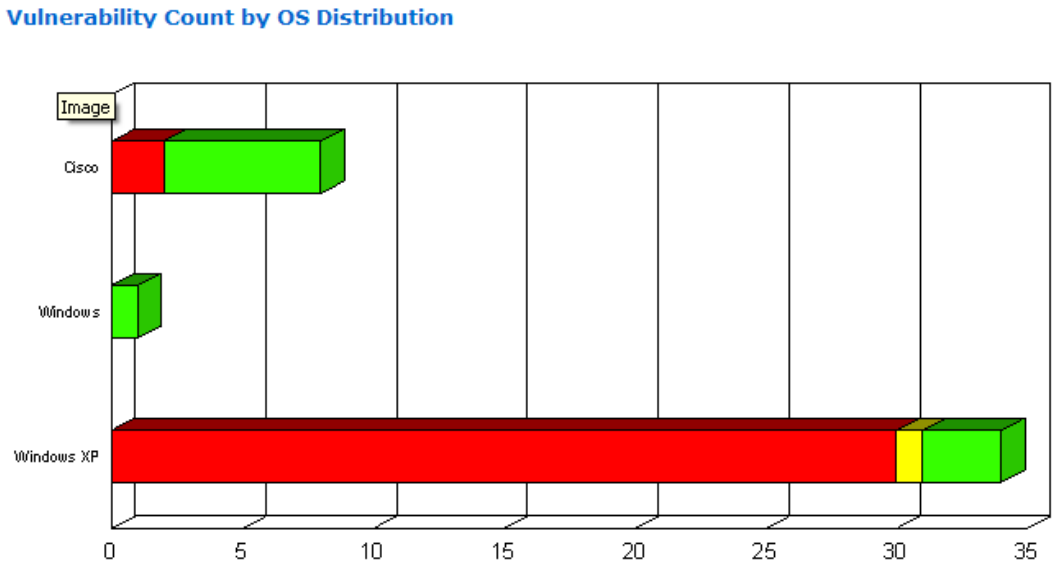
Top 10 Vulnerable Hosts (by Severity)

IP Address	Host Name	Severity		
		High	Med.	Low
192.168.1.66	TOSHIBA-KK-WINX	30	1	3
192.168.1.65	N/A	2	0	3
192.168.1.33	N/A	0	0	3
192.168.1.34	IDE6682	0	0	1

Fig. 2.2 Fig 5.5 Network Vulnerability Summary Report after Configuring Security tool

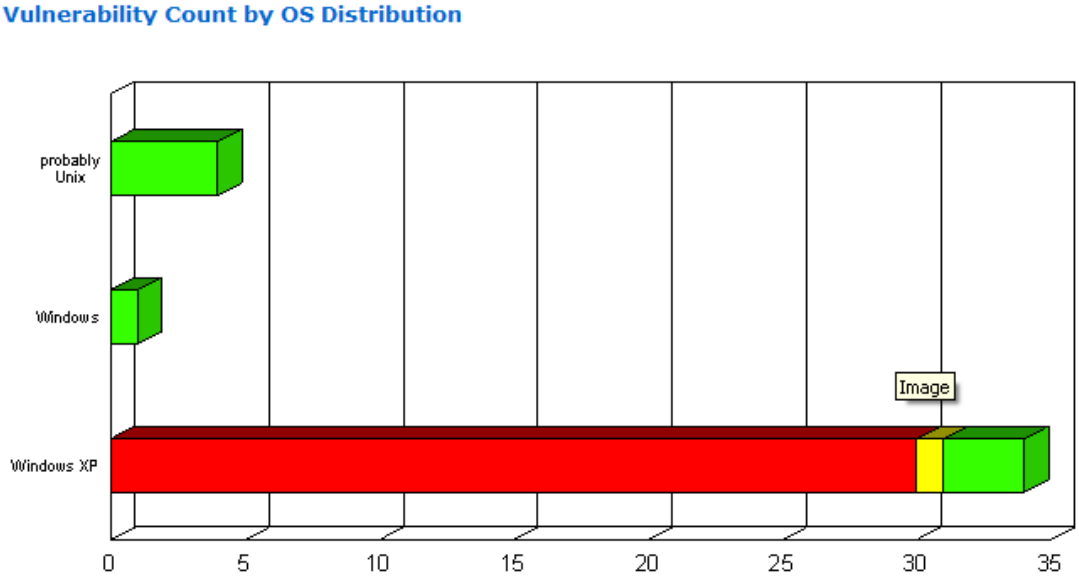
The two above two figures illustrate the difference between the severity levels in the network that we built with or without the security solution which we offer.

In the first diagram, we can see the network 192.168.1.65, which has the severity level of 2 but, in the next diagram, after configuration of security policy, the severity level has reduced to 0 in that network, which shows the increase of the security. Actually, it happens because of implementing the CISCO router security policy, based on ISO 2007.



Operating System	Severity Distribution			
	Total	High	Med.	Low
Cisco	8	2	0	6
Windows	1	0	0	1
Windows XP	34	30	1	3

Fig 5.6 Vulnerability Count by OS Distribution before Configuring Security



Operating System	Severity Distribution			
	Total	High	Med.	Low
Probably UNIX	4	0	0	4
Windows	1	0	0	1
Windows XP	34	30	1	3

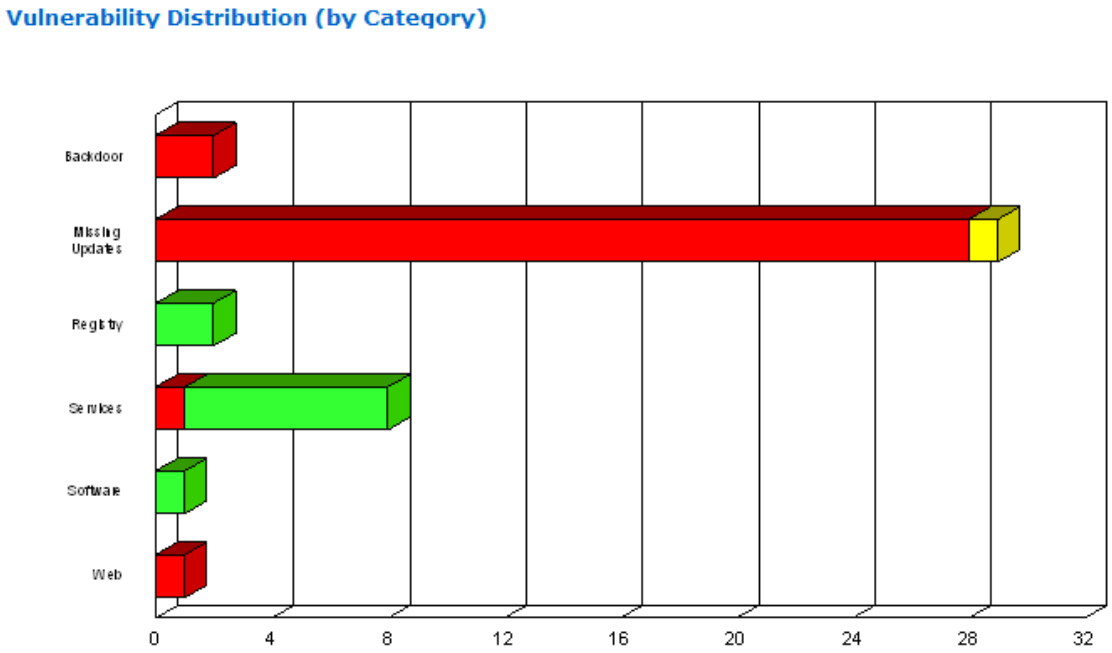
Fig 5.7 Vulnerability Count by OS Distribution after Configuring Security

The above two figures illustrate the status of the router before and after implementing ISO 27001 router security checklist**.**

Before implementing any security standard, the CISCO router has the high security risk level and**,** by considering the fact that it has the gateway role in this simulation lab, and mostly in real world, this shows the network is highly vulnerable to different kinds of threats from outside of the network or the Internet.

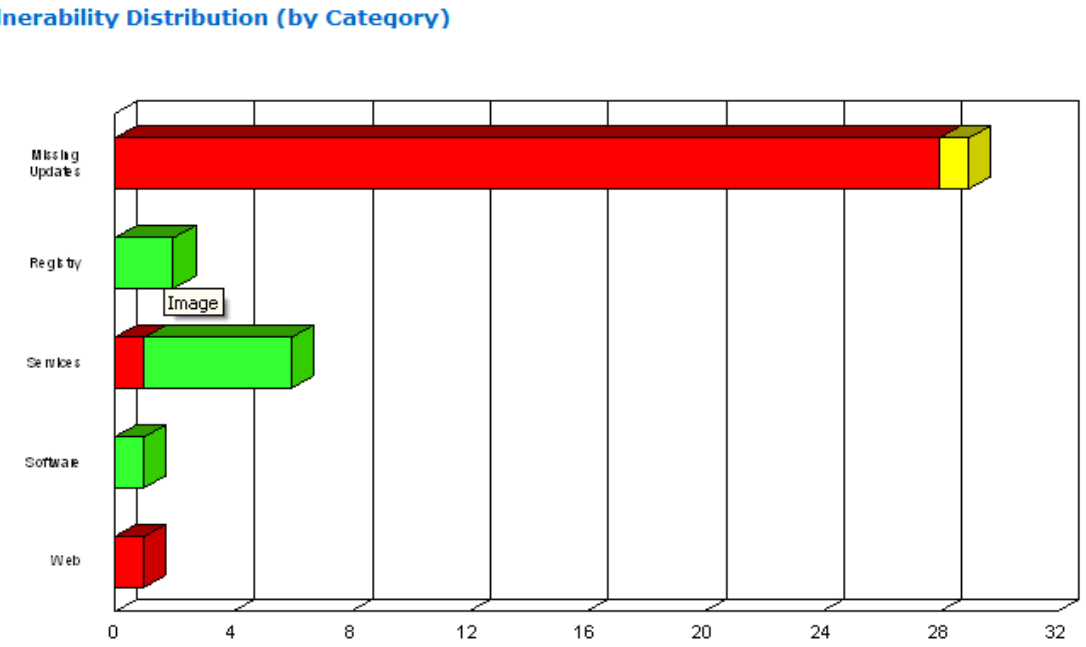
However**,** when we check the status of the security, after implementing the security policy on the router, the security risk level is considerably reduced.

Because of the security consideration, all detailed information about the CISCO router is hidden to the other network entities**,** as shown in the table. It is commonly referred to as "probably UNIX.".



Vulnerability category	Severity Distribution			
	Total	High	Med.	Low
Back door	2	2	0	0
Missing updates	29	28	1	0
Registry	2	0	0	2
Services	6	1	0	5
Software	1	0	0	1
Web	1	1	0	0

Fig 5.8 Vulnerability Distribution by category before Configuring Security Scanner



Vulnerability category	Severity Distribution			
	Total	High	Med.	Low
Missing updates	29	28	1	0
Registry	2	0	0	2
Services	6	1	0	5
Software	1	0	0	1
Web	1	1	0	0

Fig 5.9 Vulnerability Distribution by category after Configuring Security

Lastly, from the two above two figures, the results of the simulation before and after implementing the security policy, it is obvious there are backdoor entries, called “intruders”, in the simulation result. After employing and configuring the security policy, those backdoor entries are completely prohibited.

6 Conclusion

Today, whereas organizations are faced with a large range of security threats, from equipment malfunction to human errors, fraud, theft, damage, in so many countries and, according to the fact that information can exist in many forms, the protection of information from a such threats in order to ensure business continuity is a necessity for the management of the organization.

Because of the importance of the security policy to guarantee a secure system, some research organizations have been trying to find new security models which cover all the essential concepts of computer security.

It is a fact that, currently (at the time of this report), there is no specific model for network security. In 2008, Joshua Backfield and John Bambenek (from SANS Institute), by publishing a paper, have defined a possible network security model as a framework which will allows general network security to be implemented and maintained by any size of company.

The proposed network security model (NSM) is a seven layer model based on the Open Systems Interconnection Model (OSI), which has been used to teach networking and troubleshooting networking for the past 25 years. [10]

It should be mentioned that the implementation of the information security is not a one-time process; it is a routine which needs to be performed continuously.

This process can be achieved by identifying the objectives and goals of the information security in the organization, and by defining an efficiency security policy which covers these objectives and preparing checklists for all the information assets**,** based on the ISO standard series in order to implement the security policy.

More specifically, after implementing and enforcing the security policy inside of the network (as a part of information security), by using the network monitoring tools, an administrator of the network can more precisely evaluate the situation of the network security and make correct decisions to improve the level of the security inside the network against the malicious hacker who tries to gain access to any computer which is connected to the network.

To gain such a level of security, each organization needs to have setup a working group of experts to identify, design and implement the security policies**;** to evaluate the security level of the organization from time to time**;** to prepare the management report and to offer solutions for the vulnerabilities which are probably present inside the network.

Currently, this way is going to be established as a development solution to improve the security of the information inside all organizations around the world.

7 References

[1] ISO/IEC 17799:2005 – Code of practice for information security management available at: http://www.iso.org/iso/support/faqs/faqs_widely_used_standards/widely_used_standards_other/information_security.htm

[2] Sigurjon Thor Arnason and Keith D. Willett, "How to Achieve 27001 Certification", Published by CRC Press, 2007

[3] The standard of good practice available at: https://www.isfsecuritystandard.com

[4] IT management – BS 7799 available at: http://www.tech-faq.com/bs7799.shtml

[5] Introduction to ISO 27001 available at: http://www.isoqar.ir/html/iso_27001.html

[6] Ed Tittel, James Michael Stewart, Mike Chapple, "CISSP:Certified Information System Security Professional", 2nd edition, Sybex Inc, 2003

[7] Michael E. Whitman and Herbert J. Mattord, "Principle of Information Security", 2nd edition, Thomson Course Technology, 2005

[8] Matt Bishop, "Introduction to Computer Security", Addison-Wesley, 2005

[9] Dieter Gollmann, "Computer Security", Wiley, 1999

[10] Joshua Backfield, John Bambenek, "Network Security Model", SANS Institute, 2008

8 Appendix

8.1 Network Device Security Checklist based on ISO 27001

ISO 27001 Router Security Audit Checklist

Questions	Findings Yes	Findings No	ISO 27001 Control	Standard/Best Practice
Router Policy				
Is a router security policy in place?			A.5.1.1 A.11.4.1	
Disable Unneeded Services				
Are unused interfaces disabled?			A.11.4.4	Unused interfaces on the router should be disabled. Router(config-if)# shutdown
Is DNS lookups for the router turned off?			A.11.5.4 A.12.6.1	This client service is enabled by default and is not required on most routers. The following command is used to turn DNS lookup off. Router(config)#no ip domain-lookup
Is TCP small servers and UDP small servers service disabled on the router? {applicable before Cisco IOS 11.3}			A.12.6.1	These services are rarely used and hence can be disabled. This is disabled by default after Cisco IOS 11.3 Router(config)#no service tcp-small-servers Router(config)#no service udp-small-servers
Is Cisco Discovery Protocol disabled on the router?			A.11.4.4 A.12.6.1.	CDP which is used to obtain information such as the ip address, platform type of the neighboring Cisco devices should be disabled on the router if not used by any application. Router(config)# no cdp run OR Router(config-if)# no cdp enable
Is the finger service disabled on the router? {applicable before Cisco IOS 11.3}			A.11.4.4 A.11.5.4 A.12.6.1	Unauthorized persons can use the information obtained through this command for reconnaissance attacks. This service should be disabled. Router(config)#no service finger
Is Bootp server disabled on the routers?			A.11.4.4	The Bootp server service which is enabled by default allows other routers to boot from this router.

			A.11.5.4 A.12.6.1	This feature should be disabled on the router as it is rarely used on today's networks. The following command is used to disable the service. Router(config)#no ip bootp server
Is directed broadcast disabled on all interfaces? {applicable before Cisco IOS 11.3}			A.12.6.1	Directed broadcasts permit a host on one LAN segment to initiate a physical broadcast on a different LAN segment. This feature should be disabled on the router as it could be used in denial-of-service attacks. The following command is used to disable the service. Router(config-if)#no ip directed-broadcast
Is source routing disabled on the router?			A.12.6.1	Source routing is a feature that allows individual packets to specify routes. This is used in various attacks. This feature should be disabled on the router. The following command is used to disable the service. Router(config)#no ip source-route
Is Proxy ARP disabled on the router?			A.12.6.1	Proxy ARP helps in extending a LAN at layer 2 across multiple segments thereby breaking the LAN security perimeter. This feature should be disabled on the router. The following command is used to disable the service on individual interfaces. Router(config-if)#no ip proxy-arp
Is ICMP redirects disabled on the router?			A.12.6.1	The three ICMP messages that are commonly used by attackers for network mapping and diagnosis are: Host unreachable, 'Redirect' and 'Mask Reply'. Automatic generation of these messages should be disabled on all interfaces, especially those connected to untrusted networks. The following command is used to disable the service. Router(config-if)#no ip redirects Router(config-if)#no ip unreachables Router(config-if)#no ip-mask reply
Password Encryption				

Do passwords appear in encrypted form when viewed at the configuration file?			A.11.5.3	Passwords should appear encrypted when viewed through the configuration file. The following command is used to implement the same. Router(config)#service password-encryption
Authentication Settings				
Is enable secret used for the router enable mode?			A.11.5.3	The enable secret command should be enabled to implement MD5 hashed password on enable mode. Router(config)#enable secret password
Does the enable secret password match any other username password; enable password, or the enable secret password of another router in the network?			A.11.5.3	The enable secret password should be unique across each router. If the routers are too many, instead of keeping a single enable secret password for all, the password could be different for routers in different zones.
Is a Message of the Day (MOTD) banner defined?			A.11.5.1	Login banners should be used as a preventive measure against unauthorized access to the routers. Use the following command to enable a MOTD banner: Router# config t Router(config)# banner motd ^
Is the following defined on the console port: 1. Exec-timeout 2. Password			A.11.5.1 A.11.3.1	These parameters should be defined on the console port to reduce the chance of an unauthorized access on the console port. The following commands can be used to implement the same: Cisco(config)#line con 0 Cisco(config-line)#exec-timeout 5 0 Cisco(config-line)#password password Cisco(config-line)#login
Is the aux port disabled?			A.11.4.4	The aux port should be disabled if there is no business need for the same. Use the following command to disable the aux port: Router(config)#line aux 0 Router(config-line)#no exec
Is the following defined on the vty lines: 1. Exec-timeout (Yes/No) 2. Password			A.11.5.1 A.11.3.1	These parameter should be defined on the vty port to reduce the chance of an unauthorized access. Use the following to enable these parameters on the vty lines: Router(config)#line vty 0 4

				Router(config-line)#exec timeout 5 0 Router(config-line)#password *password* Router(config-line)#login Router(config-line)#transport input *protocol*
Is the vty lines restricted to certain IP Addresses only?			A.11.4.3	If the vty lines use telnet as the transport protocol, it is advisable to restrict access to certain IP Addresses only since telnet transmits data in clear text. Use the following command to restrict vty access to certain ip addresses: Router(config)#access-list 50 permit 192.168.1.x (x represents the IP address of the administrator's machine) Router(config)#access-list 50 deny any log Router(config)#line vty 0 4 Router(config-line)#access-class 50 in
According to policy, how often do router passwords (telnet, username, enable) have to be changed?			A.11.5.3	Router passwords need to be changed periodically, typically once every 4-6 months depending on the functionality of the router.
Do the router passwords meet with the required complexity as defined by the policy?			A.11.3.1	All password defined on the router should meet the following criteria: · Minimum 8 characters in length · Should be alphanumeric along with special characters (@#$%) · Should not include organization's name in it
Is SSH used for the vty lines?			A.12.3.1	SSH is a preferred protocol over Telnet for vty access since it encrypts the data while in transit on the network.
Do any applications use telnet to perform management activities such as backing up configuration?			A.10.6.1	The Telnet protocol transfers data in clear text thereby allowing an intruder to sniff valuable data such as passwords. As a remedy the following can be done: · Using secure protocols such as SSH wherever possible · Restricting access from certain workstations only · Maintaining strong passwords
Administrator Authentication				
Is authentication on the router done through: · Locally configured usernames and passwords				

· TACACS+/RADUIS server				
Is there a documented procedure for creation of users?			A.10.1.1 A.11.2.1	A documented procedure for creation of administrators on the router should exist. The procedure should address: · Approval from the department head · Recording the authorization level given to the new administrator and the duration
Does each router administrator have a unique account for himself/herself?			A.11.2.1	Each router administrator should have a unique account for him/her to maintain accountability. The following commands can be executed to create unique local usernames on the router: Router(config)#**username** username **password** password Router(config)#line vty 0 4 Router(config-line)#login local
Is login and logout tracking/command logging for the router administrators through the TACACS+ system enabled?			A.10.10.1 A.10.10.4	A detailed log of every command typed on the router as well as when an administrator logged in or out can be recorded for audit purposes. Router(config)#aaa accounting exec default start-stop group tacacs+ Router(config)aaa accounting commands 15 default start-stop group tacacs+
Are all user accounts assigned the lowest privilege level that allows them to perform their duties? (Principle of Least Privilege)			A.11.2.2	All user accounts should be assigned the lowest privilege level that allows them to perform their duties. If multiple administrators exist on the router, each administrator should be given an individual username and password and assigned the lowest privilege levels.
Management Access				
Is the http/https Server used for router management?			A.10.6.1	This service allows the router to be monitored or have its configuration modified from the web browser. If not used, this service should be disabled. Router(config)#no ip http server If this service is required, restrict access to the http/https service using access control lists. Router(config)#ip http access-class 22

				Router(config)#access-list 22 permit host *mgmt ip* Router(config)#access-list 22 deny any log
Which version of SNMP is used to manage the router?			A.10.6.1	Ideally SNMP version 3 should be used on the router since it introduces authentication in the form of a username and password and offers encryption as well. Since the SNMP process is enabled by default, it should be disabled if not used. Router(config)# no snmp-server
Is the SNMP process restricted to certain range of IP Addresses only?			A.10.6.1 A.11.4.3	If SNMP v1 or v2c is used, ACL's should be configured to limit the addresses that can send SNMP commands to the device. SNMP v1 or v2c uses the community string as the only form of authentication and is sent in clear text across the network. Router(config)#access-list 67 permit host *snmp-server* Router(config)#access-list 67 deny any log
Is the default community strings such as 'public' and 'private' changed?			A.11.2.3	Default community strings such as 'public' and 'private' should be changed immediately before bring the router on the network.
How often is the SNMP community string changed?			A.11.3.1	If SNMP v1 or v2c is being used, the SNMP community strings should be treated like root passwords by changing them often and introducing complexity in them.
Is any access list defined restricting the syslog host to receive log messages from the routers only and only administrators' systems to connect to the log host?			A.11.4.6	
Is the NTP server service used to synchronize the clocks of all the routers?			A.10.10.6	The NTP service which is disabled by default helps to synchronize clocks between networking devices thereby maintaining a consistent time which is essential for diagnostic and security alerts and log data. However if configured insecurely, it could used to corrupt the time clock of the network devices. To prevent this, restrict which devices have access to NTP. The service should also be disabled if not used.
Ingress/Egress Filtering				

Is RFC 1918 filtering implemented?			A.11.4.7	RFC 1918 addresses are meant to be used for internal networks only and have no reason to be seen on the Internet. The following access-lists should be implemented on the Internet router: Router(config)#access-list 101 deny ip 10.0.0.0 0.255.255.255 any log Router(config)#access-list 101 deny ip 172.16.0.0 0.15.255.255 any log Router(config)#access-list 101 deny ip 192.168.0.0 0.0.255.255 any log Router(config)#access-list 101 permit ip any any
Is uRPF enabled on the Cisco router?			A.11.4.7	Unicast Reverse Path Forwarding is an alternative to RFC 2827 filtering. It can enabled using the following commands: Router(config-if)#ip verify unicast reverse-path
Route Protocol Security				
Is routing protocol message authentication enabled?			A.11.4.7	Message authentication helps prevent the spoofing or modification of a valid routing protocol message.
Configuration Maintenance				
How often is the router configurations backed up?			A.10.5.1	Router configurations should be backed up periodically depending on importance and frequency of changes made to the configuration.
Is the backup moved to an off-site/DR site?			A.10.5.1	Backup copies should be maintained off-site for quick recovery during a disaster.
On the system where the configuration files are stored, is the local operating system's security mechanisms used for restricting access to the files (i.e., the machine should be password enabled and prevent unauthorized individuals from accessing the machine.)?			A.10.5.1	If a file server is used to store configuration files, the files should be restricted to authorized personnel only.
Is the TFTP protocol used to transfer configuration or image files to and from the router?			A.10.6.1	The TFTP protocol which is disabled by default transfers files in clear text and hence is unsafe to use.

If yes, · Is the TFTP process restricted to certain addresses only? · Is the TFTP service disabled when not in use?				The TFTP process should be restricted to certain addresses only (management workstations) to reduce the risk. The service should also be disabled when not in use because it allows access to certain files in the router flash.
Is there a documented procedure for backup of router configurations?			A.10.5.1	
Router Change Management				
Are all router changes and updates documented in a manner suitable for review according to a change management procedure?			A.10.1.2	
Router Redundancy				
Is there a router redundancy in cold standby or hot standby?			A.14.1.3	
Are disaster recovery procedures for the router/network documented and are they tested?			A.14.1.3 A.14.1.5	
Log monitoring and Incident Handling				
Are all attempts to any port, protocol, or service that is denied logged?			A.13.1.1	
Is the CPU utilization/memory of the router monitored?			A.10.10.2	
Is logging to a syslog server enabled on the router?			A.10.10.1 A.13.1.1	Syslog messages allows for easy troubleshooting of the network. Use the following commands to enable syslog Router(config)#logging *syslog-ip-address* Router(config)#service timestamps log datetime localtime msec show-timezone
Are procedures for audit log review generated by the router documented and followed?			A.10.1.1	
How often is the router logs (covering administrator access /access control) reviewed?			A.10.10.1 A.10.10.2 A.10.10.5	
Are reports and analyses carried out based on the log messages?			A.13.2.2	
What is the course of action to be followed if any malicious incident is			A.13.2.1	

noticed?				
Security Updates				
Is the network engineer aware of the latest vulnerabilities that could affect the router?			A.6.1.7 A.12.6.1	The network engineer should receive periodic updates on the vulnerabilities and patches affecting the router.

source: iso27001security.com

8.2 Router Configuration

```
Router#show running-config
Building configuration...


hostname Router


!
!
no ip bootp server
no ip domain lookup
ip host PAGENT-SECURITY-V3 97.32.43.85 87.84.0.0
!
multilink bundle-name authenticated
!
!
voice-card 0
 no dspfarm
!
!


!

!
!
!

!
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/0.1
!
interface FastEthernet0/1
no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/1.1
 encapsulation dot1Q 1 native
```

```
!
interface FastEthernet0/1.2
 encapsulation dot1Q 2
 ip address 192.168.1.33 255.255.255.224
!
interface FastEthernet0/1.3
 encapsulation dot1Q 3
 ip address 192.168.1.65 255.255.255.224

!
interface lo 0
ip add              172.16.1.1 255.255.255.0

!
interface Serial0/0/0

!
interface Serial0/0/1

!
!

!
!
control-plane
!
!
!

!

!
!
end

Router#
```

8.3 Switch Configuration

```
Switch#show running-config
Building configuration...

Current configuration : 1350 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch
!
!
no aaa new-model
system mtu routing 1500
ip subnet-zero
!
!
!
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
 vlan internal allocation policy ascending
 !
 interface FastEthernet0/1
  switchport mode trunk
 !
 interface FastEthernet0/2
  switchport access vlan 2
  switchport mode access
 !
 interface FastEthernet0/3
  switchport access vlan 3
  switchport mode access
 !
 interface FastEthernet0/4
 !
 interface FastEthernet0/5
 !
 interface FastEthernet0/6
 !
```

```
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
ip http server
!
```

```
 control-plane
 !
 !
 line con 0
 line vty 5 14
line vty 15
 login
!
end

Switch#
```