NEAR EAST UVIVERSITY

Faculty of Engineering

Department of Electrical and Electronics Engineering

NETWORK SECURITY

Graduation Project
EE- 400

Student: Ayman Abu-Khurma (20034232)

Supervisor: Dr.Jamal Abu-Husna

Nicosia-2008

ACKNOWLEDGEMENT

First of all, I would like to thanks Allah {God} for guiding me through my study.

I feel proud to pay my special regards to my project advisor ".Dr. jamal abu-Husna". He gave me too much information and did his best of efforts to make me able to complete my project. He has special respect and Devine place in my hearts.

More over I want to pay special regards to my family. They encouraged me in crises. I shall never forget their sacrifices for my education so i can start my successful life and enjoy it as they are expecting. I am nothing without their prayers.

I want to honor all those persons who have supported and helped me in my project and send to them the best of regards and acknowledge. Also my special thanks to all my friends who gave me their precious time to complete my project. Also my especial thanks go to my friends, Omer Touqan, yahea daban, zeyad Al-kayaly Mohammad al-smadi, Abedalazeez Al-natsheh, Marwan Shraideh, Haidar Al-agha, Mohammad sabri, Mohammad Al-sheab, zaqaria Abu-khurma and all the other friends.

At the end I am again thankful to all persons who helped and encouraged me to complete my project, and complete the first step of my future life.

CONTENTS

ABSTRACT

The aim of this project makes security to network in order to prevent any risk through that network & communication to accomplish successful work.

Security controls and safeguards must be implemented to reduce such risks this should take place in all levels of the network and all stages of network Development The network should be designed with security in mind and be easy to Manage. The network should be safeguarded against current vulnerabilities and regularly tested for new Vulnerabilities and threats. Risks should be mitigated and attacks logged so as to provide forensic evidence.

Introduction

The requirements of information security have undergone three major changes in the last decades the first major change was the introduction of the computer the need for protecting files and information became evident. Collection of tools designed to protect data and to avoid hacker attacks has the generic name computer security. The second major change was the introduction of distributed systems, networks and communication facilities for data communication. Network security measures are needed to protect Data during transmission. The third change is the current, rapid development of wireless networks and mobile communications. Wireless security is therefore of high priority today.

1. NETWORK

1.1 Introduction

Communication may be broadly defined as the transfer of information from one point to another. When the information is to be conveyed over any distance a communication system is usually required. Within a communication system the information transfer is frequently achieved by superimposing or modulating the information on to an electromagnetic wave which acts as a carrier for the information signal. This modulated carrier is then transmitted to the required destination where it is received and the original information signal is obtained by demodulation. Sophisticated technique have been developed for this process using electromagnetic carrier waves operating at radio frequencies as well as microwave and millimeter wave frequencies. However, communication may also be achieved using an electromagnetic carrier which is selected from the optical range of frequencies.

1.2 Historical Development

The use or visible optical carrier wave or light for communication has been common for many years. Simple systems such as signal fires, reflecting mirrors and more recently. Signalling lamps have provided successful if limited, information transfer. Moreover, as early as 1880 Alexander Graham bell reported the transmission of speech using a light beam. The photo phone proposed by Bell just four years after the invention of the telephone modulated sunlight with a diaphragm giving speech transmission over a distance of 200m However although some investigation of optical communication continued in the early part of the twentieth century its use was limited to mobile, low capacity communication links This was due to both the lack of suitable light sources and the problem that light transmission in the atmosphere is restricted to line of sight and is severely affected by disturbances such as rain, snow, fog dust and atmospheric turbulence Nevertheless, tower frequency and hence longer wavelength electromagnetic waves (i.e. radio and microwave) proved suitable carriers for information transfer in the atmosphere, being far less affected by these atmospheric conditions Depending on their wavelengths these electromagnetic carriers can be transmitted over considerable distances but are limited in the amount of information they can convey by their frequencies (i.e. the

information-carrying capacity is directly related to the bandwidth or frequency extent of the modulated carrier which is generally limited to a fixed fraction of the carrier frequency).In theory, the greater the carrier frequency, the larger the available transmission bandwidth and thus the information-carrying capacity of the communication system. For this reason radio communication was a developed to higher frequency (i.e. VHF and UHF) leading to the introduction of the even higher frequency microwave and, latterly, millimetre wave transmission. The relative frequencies and wavelengths of these types of electromagnetic wave can be observed from the electromagnetic spectrum In this context it also be noted that communication at optical frequencies offers an increase in the potential usable bandwidth by a factor of around 10^4 over high frequency microwave transmission. An additional benefit of the use of. high carrier frequencies is the general ability of the communication system to communication system to concentrate the available power within the transmitted electromagnetic wave, thus giving an improved system performance. a renewed interest in optical communication was stimulated in the early 1960s with the invention of the laser his device provided a powerful coherent light source together with the possibility of modulation at high frequency In addition, the low beam divergence of the laser made enhanced free space optical transmission a practical possibility. However, the previously mentioned constraints of light transmission in the atmosphere tended to restrict these systems to short distance applications. Nevertheless, despite the problems some modest free space optical communication links have been implemented for applications such as the linking of a television camera to a base vehicle and for data links of a few hundred meters between buildings There is also some interest in optical communication between satellites in outer space using similar techniques Although the use of the laser for free space optical communication proved some what limited, the invention of the laser instigated a tremendous research effort into the study of optical components to achieve reliable information transfer using a light wave carrier The proposals for optical communication via dielectric waveguide or optical fibres fabricated from glass to avoid degradation of the optical signal by the atmosphere were made almost simultaneously in 1966 by Kao, Hockham, and Werts Such systems were viewed as a replacement for coaxial cable or carrier transmission systems. Initially the optical fibres exhibited very high attenuation (i.e. 1000dB/ km) and were therefore not comparable with the coaxial cables they were to replace (i.e. 5 to 10dB/ km).There were also serious problems involved in jointing the fiber cables in a satisfactory manner to achieve low loss and to enable the

process to be performed relatively easily and repeatedly in the field. Nevertheless within the space of ten years optical fiber losses were reduced to below 5 db/ km and suitable low loss jointing techniques were perfected.In parallel with the development of the fiber waveguide attention was also focused on the other optical components which would constitute the optical fiber communication system. Since optical frequencies are accompanied by extremely small wavelengths the development of all these optical components essentially required a new technology. Thus semiconductor optical sources (i.e. injection lasers and light emitting diodes) and detectors (i.e. photodiodes and to a certain extent phototransistors) compatible in size with optical fibers were designed and fabricated to enable successful implementation of the optical fiber system. Initially the semiconductor lasers exhibited very short lifetimes or at best a few' hours. but significant advances in the device structure enabled lifetime greater than 1000 hr I and 7000 hr to be obtained by 1973 and 1977 respectively. These devices were originally fabricated from alloys of gallium arsenide (AlGaAs) which emitted in the near infrared between 0.8 and 0.9μ m.To obtain both the low loss and low dispersion at the same operating wavelength, new advanced single-mode fiber structures have been realized: namely, dispersion shifted and dispersion flattened fibers. Hence developments in fiber technology have continued rapidly over recent years, encompassing other specialist fiber types such a polarization maintaining fibers, as well as glass materials for even longer wavelength operation in the mid-infrared (2 to 5μm) and far-infrared (8 to 12μm) regions. In addition, the implementation of associated fiber components (splices, connector's couplers, etc) and Active optoelectronic devices (sources, detectors, amplifiers, etc.) have also moved forward with such speed that optical fiber communication technology would seem to have reached a stage of maturity within its development path Therefore high-performance reliable optical fiber communication systems are now widely deployed both within telecommunications networks and many other more localized communication application areas.

1.3 Research on the Communication Process

Much of the research on the communication process in work settings has focused on factors that can increase or decrease its effectiveness. Among the factors that can affect the flow of communication from sender to receiver are source factors, channel factors and audience factors.

1.3.1 Source Factors

These are the characteristics of the sender. One such factor is status. Generally, the higher the organizational status of the sender, the more likely the communication will be listened to and acted upon, another source factor is credibility. If the source is trusted, it is more likely that the message will receive attention a final factor is the encoding skill of the sender. These skills include the ability to speak and write clearly and to select the appropriate channel for transmitting the information.

1.3.2 Channel Factors

These are the characteristics of the vehicle of transmission of a message that affect communication. Selection of the proper channel can have an important effect on the accurate flow of communication; the channel selected can also affect the impact of the message for example, face-to-face reprimand from a supervisor might carry more weight than the same reprimand conveyed over the telephone, whenever possible, using multiple channels to present complicated information will increase the likelihood that it will be attended to and retained Semantic problems are common channel factors that can lead to a breakdown in communication. These problems may arise because different people may interpret the meanings of words differently. Semantic problems may arise because of the use of technical language or jargon, the special language that develops within a specific work environment. Jargon is typically filled with abbreviated words, acronyms and slang while jargon serves the purpose of speeding up communication between those who speak the language, it can create problems when the receiver is not "fluent" in its use. The use of jargon can also present problems when a team of workers is from different professional disciplines, all of which may use different jargon. The choice of channel can affect important work-related outcomes like job-satisfaction. Muchinsky (1977) conducted a survey using questionnaires in a number of workplaces in America and found that the frequency of face-to-face communication between supervisors and subordinates was positively related to the workers' job satisfaction, while the frequently written communications was negatively correlated with satisfaction.

1.3.3 Audience Factors

These are elements related to the receiver, such as the attention span and perceptual abilities, For example. It is essential that training information is presented at a level that matches the audience's ability to understand it. Moreover, it may be critical to consider the attention span of the target audience All-day training sessions may be appropriate for management trainees who are used to long sessions, but the attention of assembly-line workers may be lost after an hour because of their unfamiliarity with the format. The relationship to the sender may also affect the communication process. For example if the receiver is subordinate to the sender, the message may be better attended to because people are supposed to listen to their bosses. Finally, decoding skills may influence the effectiveness of communication. Research has shown that effective managers have good decoding skills in listening and responding to the needs and concerns of their subordinates. In fact, because most of the communication in work settings involves spoken communications, oral decoding skills, often referred to as listening skills, are considered to be the most effective decoding skills of all

1.4 Communication Networks and Cycles

1.4.1 The Flow of Communication In Organizations

Messages flow through communication lines and networks, giving life to the work of organizations. The communication flow in work organizations is usually classified into three types: it can flow downward through the organizational hierarchy; upward, through the same chain of command; or it can flow laterally from colleague to colleague.

1.4.2 Downward Communication

This consists of messages sent from superiors to subordinates.

Most commonly they are:

1. Instructions or directions concerning job-performance
2. Information about organizational procedures and policies
3. Feedback to the subordinates concerning job performance
4. Information to assist in the co-ordination of work tasks.

While much formal communication in organizations is downward, research indicates that most organizations still do not have enough of this communication. A number of studies

indicate that workers would like more information from their superiors about work procedures and about what is happening elsewhere in the organization. It also appears that certain types of downward communication may be particularly limited, such as feedback concerning work performance. This is especially true in companies that fail to conduct regular performance appraisals.

1.4.3 Upward Communication

This is the flow of messages from the lower levels of the organization to the upper levels It most typically consists of information managers need to perform their jobs, such as feedback concerning the status of lower-level operations, which could include reports of production output or information about any problems. The upward flow of information is critical for managers, who must use this information to make important work-related decisions. Upward communication can also involve complaints and suggestions for improvement from lower-level workers and is significant because it gives subordinates some input into the functioning of the Organization.

1.4.4 Lateral Communication

This is the flow of communication between people who are on the same level in an organization, and is particularly important when co-workers must co-ordinates their activities in order to accomplish a goal. Lateral communication can also occur between two or more departments in an organization e.g. between the production and quality-control departments. Lateral communication allows for the sharing of news and information and helps develop interpersonal relationships. But too much socializing on the job can detract from effective job performance.

1.5 Communication Network

When we look beyond two-person communication to the linkages among work groups departmental or organizational members, we are concerned with communication networks which are systems of communication lines linking various senders and receivers. The flow of information is regulated by several factors: the proximity of workers to one another, the rules governing who communicates with whom, the status hierarchy, and other elements such as job assignments and duties. Communication networks are formal and follow the organigram within an organization. Five major types have been studied in depth.

Centralized networks (Chain, Y, and Wheel) where the flow is centralized or directed through specific members. Decentralized networks, (Circle, All-Channel) where the communication flow can originate at any point and does not have to be directed through certain central group members. Centralized networks are governed by members' status within the organization; decentralized networks typically are not. Often, decentralized networks are controlled by factors such as proximity, personal preference.

1.5.1 Centralized Networks

The first centralized network – the chain – represents a five-member status hierarchy a message originates at the top or bottom of the chain and works its way upward or downward. The flow of information in a chain system is relatively slow process, but it is direct with all members in the hierarchy being made aware of the message since it must pass through each link. A related communication network is the Y (or inverted Y). It is also a hierarchical network and represents four levels of status within the organization, but its last level of communication involves more than one person. Both chain and Y are similar in speed of communication and formality of who communicates with whom The wheel network involves two status levels: a higher status member (usually a work supervisor) and four lower-lever members. The higher status member is the centre or hub through which all messages must pass. There is no direct communication between lower-level members. An example might be a sales manager and his four salespersons in the field.

1.5.2 Decentralized Networks

The circle network represents communication between members who are immediately accessible to each other, such as workers positioned side by side on an assembly line. Because messages can originate anywhere and no rules govern the direction in which messages can be sent, it can be difficult to trace the original source of a message. It has a fairly quick rate of transmission. An all-channel network allows complete freedom among communication links. Any member can freely communicate with any other member and all members are accessible to each other. Communication can be very rapid and there is maximum opportunity for feedback Boards of directors, problem-solving task forces and employees working as a team is examples of this form of communication.

1.5.3 Research

There has been extensive research on communication networks; most of it has been conducted in laboratory settings the results of these studies indicate that each of the different networks has different strengths and weaknesses Centralized networks are faster and make fewer errors in dealing with simple repetitive tasks than do decentralized networks. Decentralized networks, on the other hand, are better at dealing with complex tasks such as problem solving. In general, straightforward, repetitive tasks, such as assembly or manufacturing work, tend to operate well with a centralized communication network, while creative tasks, such as group working on a product advertising campaign, are best accomplished using decentralized networks One reason why centralized networks may have difficulty in solving complex problems is because of information overload on the central person. Because messages cannot be passed on intact to the various members efficiently and quickly, group performance suffers the type of network can also affect the satisfaction of network members. Because of restriction in who can initiate and who can communicate with whom, members in centralized networks have lower levels of satisfaction (Shaw, 1964). More specifically, the persons in the central position tend to have high levels of satisfaction due to their role, whereas the no central members have extremely low satisfaction some of the research has been criticized for oversimplifying the process. Evidence suggests that in the workplace, the differences in the speed and efficiency among the various networks may disappear over time as the group involved learns to adjust to the required pattern (Burgess, 1968). Because most of the research has been conducted in laboratory settings, there has been some concern about whether these studies will generalize to actual workplaces, although the findings do allow us to model (although simplistically) the communication networks in work organizations.

1.6 Formal and Informal Lines of Communication

1.6.1 The Hierarchy versus The Grapevine

In looking at communication networks we have considered formal lines of communication However, while every organization possesses formal lines of communication each also has informal lines known as the grapevine The grapevine can follow any course through a network and because much of the information flow in an organization is informal the

organizational grapevine is an important element of study for psychologists While formal lines of communication follow the company's organizational chart; informal lines of communication are illustrated by a sociogram,these represent other organizational members with whom members typically interact.Baird (1977) suggests that three factors typically determine the pattern of communication links that form a grapevine: friendship, usage and efficiency We pass information to our friends, we communicate with those we like and avoid communicating with those we don't like. Friendship is perhaps the most important factor that holds the grapevine together. Workers who come into contact with each other for job-related reasons are more likely to start sharing information informally (smoking rooms or areas may be an interesting source of research). Finally, the grapevine sometimes develops because it is easier and more efficient for workers to follow their own informal networks rather than formal lines of communication. In addition to being a substitute network for formal lines of communication; the grapevine also serves a vital function in maintaining social relationships among workers. Formal lines of communication tend to be task-related; the grapevine serves to meet the social needs of workers-long deemed to be important to workers. The grapevine can serve to bring workers together and encourage them to develop a sense of unity and commitment to the workgroup and organization. This can play big role in reducing absenteeism and turnover rates (Baird, 1977). The grapevine also serves to reiterate important messages sent through formal lines of communication. While the grapevine serves many important functions it can also be perceived as having a somewhat negative function: the transmission of rumours.

1.6.2 Rumours

These involve information which is presented as fact, but which may actually be true or false. Rumours are based on such things as employee expectations or wishful thinking. Many managers are concerned about the grapevine and attempt to stifle it, because they believe it to be a source of rumours which may damage the company. However, research indicates that this is a myth. The transmission of false rumours via the grapevine is actually relatively rare, and estimates indicate that the grapevine is accurate over 80% of the time. This compares well with the accuracy of messages sent over formal communication lines!

1.7 Improving Communication Flow

Increasing upward flow in organizations: Several strategies that can increase upward Communication:

- Employee Suggestion Schemes: There are a variety of ways in which workers can submit ideas usually ideas are encouraged by some sort of incentive or bonus scheme based on the amount of savings the suggestion produces. This can lead to innovations but a drawback is that the suggestion system may be used to voice complaints about conditions management is unable to change
- Grievance Systems: These are designed to change existing negative situations and must be handled delicately to protect the employee from retribution Company officials must acknowledge the receipt of the grievance to keep the channels of communication open and make it clear what action has been taken.
- Open-Door Policies: This involves setting aside times when employees can go directly to managers to discuss whatever is on their minds this bypasses the intermediate steps in the upward organizational chain ensuring important messages do indeed get to the top intact. An obvious drawback is the danger of using manager's time on what may be a trivial matter.
- Employee Surveys: This is a quick way to measure employee attitudes in order to target problem areas or to solicit ideas for improvement. Because they have the benefit of anonymity, workers can respond honestly without fear of reprisal. Feedback from management is essential to give the respondents the impression that it was not a waste of time.

1.8 The Stages of Communication Flow

1.8.1 Source

As the source of the message, you need to be clear about why you're communicating, and what you want to communicate. You also need to be confident that the information you're communicating is useful and accurate.

1.8.2 Encoding

Senders need to pay attention to the choice of an appropriate channel and avoid the use of jargon.

1.8.3 Transmission

Changes in the sense of a message may occur during transmission through information being omitted, distorted or filtered out. What gets maintained are the important or outstanding features? If messages are incomplete, people will fill in any missing parts with what appears to rationalise the message. Hence, improvements to communication include dealing with any factors that produce loss of clarity such as noise, haste, over-reliance on memory. Complex messages delivered orally need to be followed up with written material. (See figure 1.1 and 1.2 stage of communication).

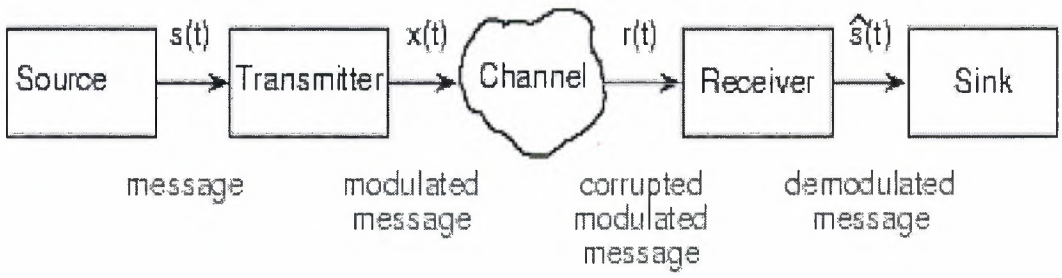

Figure 1.1 Structure of Communication System

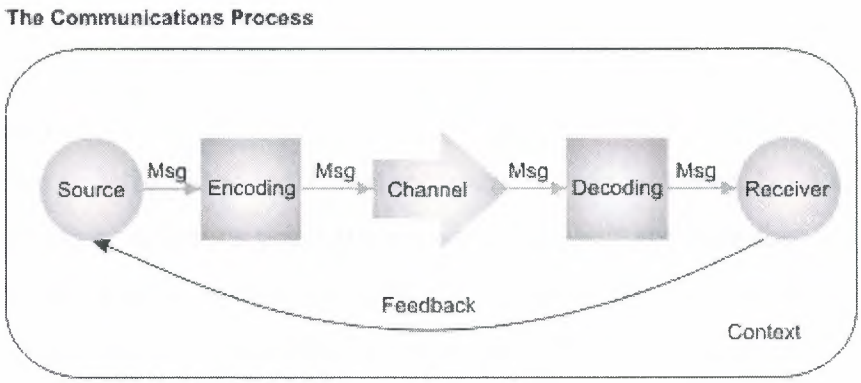

Figure 1.2 Communication Process

1.8.4 Reception

The state and context of the receiver is all important in the efficient reception of a message. Effective communication will take account of this factor.

1.8.5 Decoding

Receivers' expectations can seriously distort the content of any message they decode. People rely on their schemas when decoding information. Hence, information needs to be put into a clear context before moving onto detail

1.8.6 Feedback

Feedback is essential for effective communication to have taken place in face-to-face contact, this is immediate, but with written communication, replies (which may be tedious) are essential for the communication process to have been effectively completed.

1.8.7 Message

The message is the information that you want to communicate.

1.8.8 Channel

Messages are conveyed through channels, with verbal including face-to-face meetings, telephone and videoconferencing; and written including letters, emails, memos and reports, Different channels have different strengths and weaknesses For example, it's not particularly effective to give a long list of directions verbally, while you'll quickly cause problems if you criticize someone strongly by email.

1.8.9 Receiver

Your message is delivered to individual members of your audience. No doubt, you have in mind the actions or reactions you hope your message will get from this audience. Keep in mind, though, that each of these individuals enters into the communication process with ideas and feelings that will undoubtedly influence their understanding of your message, and their response. To be a successful communicator, you should consider these before delivering your message, and act appropriately.

1.9 Summary

In this chapter, we explained research on communication process, communication network and cycle, communication network, Formal and Informal Lines of Communication, Improving Communication Flow, and The Stages of Communication Flow.

2. NETWORK SECURITY

2.1 Introduction

As new end-user services are introduced in today's converged multi-service networks telecom network security becomes more of an issue for operators and demand from public users, enterprises and government agencies. If not given the appropriate attention, the technologies that deliver these services may actually degrade the security of the network over which the service is delivered. Security breaches, whether they disrupt services or compromise information, cause financial losses. Examples are financial penalties for failing to maintain performance agreements, lost revenue caused by network disruptions, lost consumer loyalty, ill will, lawsuits, and industrial espionage. Moreover, individual public users, agencies and corporations are demanding highly secure connections to telecom networks; service providers with roaming agreements want secure interfaces with their roaming partners and insurance providers, always conscious of risk, are insisting upon stringent security. Telecom Network Security Awareness and acting proactively can, apart from reducing risk, also reduce Operational cost. The operator needs a trustworthy security story if they are to be taken seriously in the marketplace. The Ericsson approach is to address security at an early stage in a structured Manner; from procedural, personnel, physical and technical points of view. In this Way a secure, cost Effective security solution can be established and maintained to protect sensitive information and network operator business.

2.2 What Causes Problems In Telecom Networks?

Traditionally, telecom networks refer to the infrastructure required to establish an End-to-end transfer of analogue or digital information. This comprised the transmission and switching infrastructure. Today, the infrastructure is divided into layers in order to achieve higher level of service integration. The new infrastructure supports fixed and wireless network services. Telecom networks distinguish between traffic (e.g., voice, data and multimedia) and control (signaling). A different layer, called connectivity network, is

defined for traffic, and another layer, called control layer, is defined for signaling. As more applications and services appeared, another layer was introduced, the service layer. Operations& Maintenance (O&M) networks require high security, and that leads to another sub layer within the core network. With all the advantages that we can mention about the integrated layered architecture of telecom networks, we should not overlook the increasing number of security concerns that apply to all types of services and all levels of the telecom network access networks are subject to denial-of-service attacks and various unauthorized-access attacks. Fixed networks suffer from clip-on access and associated fraud, as well as violation of privacy. Wireless networks do not require physical access, and are even more exposed. Mobility adds other vulnerabilities and threats, including SIM card cloning, subscription frauds and man-in-the-middle attacks and so on Core networks have a multitude of interconnection points, which mean different security requirements and possible exposure to a wide range of threats and vulnerabilities Attacks on the core would lead to larger impacts on the different services and stakeholders, such as end users, service and application providers, and the operator itself Stealing passwords and accessing the management ports, attacking the signaling layer, targeting databases of subscribers, HLRs, OSSs network elements, gateways, and application servers could lead to security Violations, fraud and service interruption As networks grow and become increasingly complex, the risk of holes in security due to configuration and/or design mistakes increases. As increasingly more business critical applications rely on the availability of the networks, the exposure to loss is also becoming drastically higher. Users expect reliability in all transactions, independent of access, and guaranteed connection quality. From a security point of view, the user expects no viruses, no worms, no fraud, nobody listening in, and the ability to know who requests a communication session.

2.3 Structured Approaches To Security

2.3.1 Identifying Needed Security Services And Functions

Security solution development begins with threat-risk analysis. It is required to identify assets, threats and vulnerabilities; rank the different assets in the order of their importance for the business, and evaluate different alternatives to handle the Risk.

The risks are then grouped into categories such as:

- Must be minimized/eliminated
- Should be minimized/eliminated
- Acceptable.

This information enables decision-makers to capture requirements and to specify the Implementation of security services and functions.

2.3.2 Security Policy

A security policy should be a statement of management intent, supporting the goals and principles of information security in line with the business strategy and objectives. The policy performs several functions that help ensure the effectiveness of whatever security strategy the organization pursues. Specifically, it:

- Defines information security and its overall objectives an scope.
- Defines acceptable security practices; a framework for setting control objectives. And controls, including the structure of risk assessment and risk management
- Establishes roles and responsibilities definition of general and specific responsibilities for information-security management including reporting information security incidents.

Briefly explains the security policies, principles, standards, and compliance requirements of particular importance to the organization, including:

- Compliance with legislative, regulatory, and contractual requirements
- Security education, training, and awareness requirements
- Business continuity management. The security policy framework should be the "Hub" around which all security-related services and functions evolve.

2.3.3 Network Security Architecture Reference Model

To provide adequate security, it is important to be able to model the mobile network and analyze the threats to assets. The following three-plane architecture (based on the international standard X.805) provides a useful and simple way of capturing relevant information. This model consists of four architectural components: separate security planes, security layers, security services, and security policies & principles (see figure 2.1).

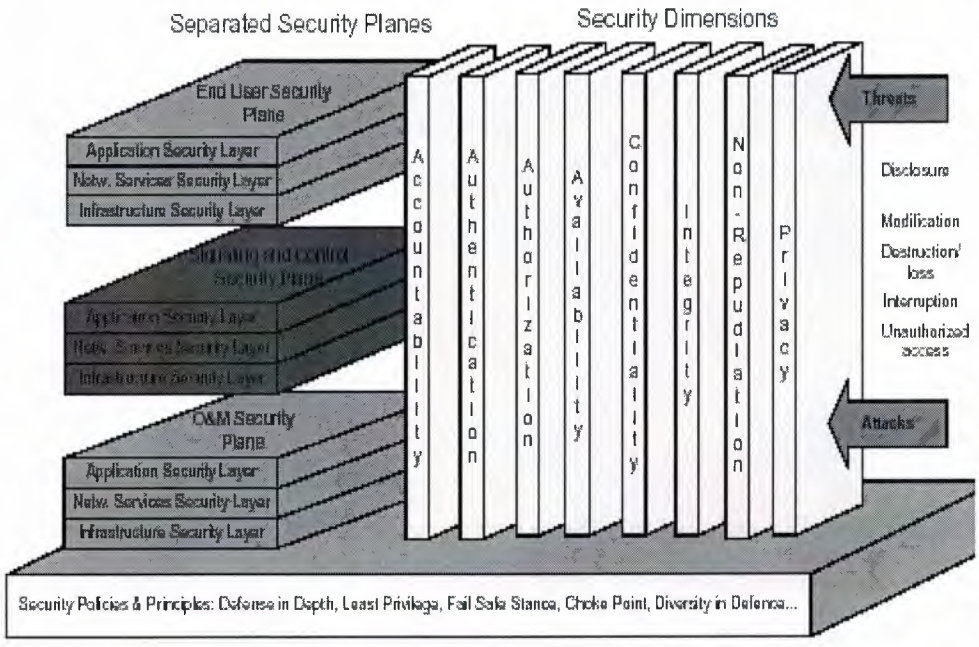

Figure 2.1 Network Security Architecture Model

2.3.4 Security Planes

Networks should be designed in such a way that events on one security plane are kept totally isolated from the other security planes. The concept of security planes provides the ability to differentiate and address security concerns independently. The End-User Security Plane addresses security of access and use of the service provider's network by customers. This plane also represents actual end-user data flows. The Signaling and Control Security Plane covers protection of the activities that enables the efficient delivery of information,

services and applications across the network. The O&M Security Plane covers the protection of operation and maintenance functions.

2.3.5 Security Dimensions

The security dimensions are system aspects which run through all security solutions. However, security solutions and mechanisms are used for implementing the security dimensions. All security dimensions should be evaluated in each security plane/layer intersection point. The most common ones are:

- Authentication
- Authorization
- Accountability
- Availability
- Confidentiality
- Integrity
- Non-repudiation and privacy

2.3.6 Security Policies And Principles

To enhance protection of the network, specific security principles and best practices are commonly used. Probably the most important one is the defense-in-depth principle: employ several security mechanisms and security layers to provide protection. If one of the mechanisms or layers fails, the other mechanisms and layers are still in place to provide sufficient protection. This principle is commonly used to protect the perimeter of a site, as depicted earlier in (Figure 2.1) the least privilege is another fundamental security principle. It means that an entity should only have the privileges it needs to perform its tasks. This is of utmost importance when considering node protection. The services running on a node should have only the privileges they need to provide the service and the node should not be running any unnecessary services. Systems and nodes should also implement the fail-safe principle. This means that when the system or node fails, it should fail without harmful side effects. Sometimes, the diversity-of-defense principle might also be useful. This principle is based on using different types of systems to provide a certain kind of protection. If one of the systems contains vulnerability, the other systems might not have that vulnerability

and the impact of the vulnerability is thus mitigated. A choke point forces attackers to use a narrow channel, which can be monitored and controlled. In network security the proper perimeter protection for the site is such a choke point; anyone attacking the site from the outside will have to go through that channel, which should be defended against such attacks.

2.4 Managing Security

To be able to make sound security judgments, both the particular business context and the networking environment must be fully understood. To support the whole telecom system life cycle, from end-to-end, the following operations have to be undertaken:

- Business Continuity Management
- Network Security Design
- Network Configuration / Integration
- Network Security Audits
- Network Security Implementation
- Fraud Management.

2.4.1 Common Principles

The security operations address

- Risk Management: all network operation implies a certain risk that must be accepted avoided, reduced or transferred.
- Business Continuity: the operator's critical processes and information should be protected from disclosure and/or disruption.
- Lowering operator costs: well thought-out security solutions provide a payback in terms of reduced operating costs, reduced risk of fraud, a reduced risk of critical security-related network outages and potentially less churn. The following chapter describes how the different sub-operations complement each other and fit into the "Security Wheel" concept, forming continuous security management.

2.4.2 The Security Wheel

This industry-standard model has been chosen to illustrate where security Management fits in, and how all security activities in a network must evolve around the security policy; the concept sees network security as a continuing process built around a

Corporate security policy. This process is divided into the stages:

- Implement network security
- Monitor network and respond to incidents
- Test the security of the network
- Improve network security. Implement network security –Security devices such as Perimeter nodes, VPN devices, firewalls, Intrusion Detection/Prevention Systems (IDS/IPS) and authentication devices are planned; configured and integrated the purpose is to prevent activities that the policy has defined as threats. Monitor/Respond the implemented security policy is validated using intrusion Detection, as well as log and other auditing techniques, to watch for violations Test the effectiveness of the policy should be evaluated at regular intervals through security audits, vulnerability scanning and/or penetration tests. Manage/Improve

Information gathered from previous steps is analyzed (see figure 2.2) and used Together with developments in the security market to improve the policy, moving around the circle to the first step again.

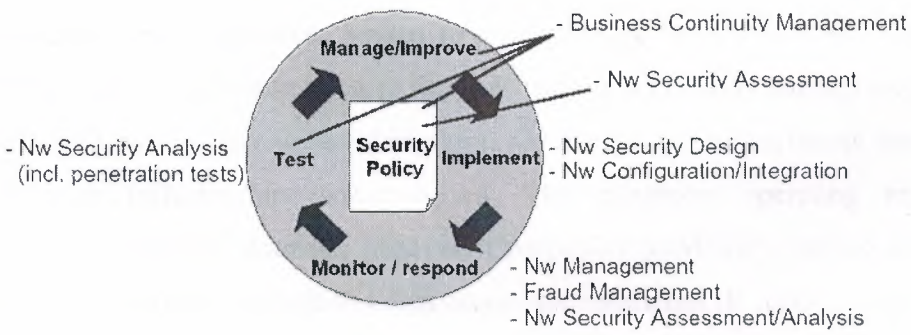

Figure 2.2 The Security Wheel model

2.4.3 Security – A continuous Process

Security Policy – Is, together with the Risk Analysis, the most fundamental part of any company's security/business continuity process. These can be checked and/or developed as a part of either the security assessment service or the business continuity service. Business Continuity also includes such aspects as, for example, crisis management, disaster recovery, and organization resiliency. Risk Analysis and Readiness planning is of utmost importance in guaranteeing the safe launch of a new service. Implement Network Security – Network Security Design ensures that security is implemented according to best telecom practices, and the level planned for in the Security policy. Also, configuration and integration must be performed in the most secure manner possible, and according to plans. Monitor/Respond – Network Management personnel monitor logs, while Intrusion Detection System real-time alarms detect any signs of attempted policy violations. Fraud-management processes and solutions instantly detect malicious end-user behavior. The network security organization must be continuously updated with the latest methodology to perform IDS/IPS tuning, log analysis and computer forensics.

2.5 Telephony Security Networks

Telephony networks typically interface to subscribers through a shallow and well-defined Interface. After the introduction of out-of-band control technology based on Signaling Contact person. System 7 (SS7) in 1970s, the number of security incidents involving the core telephone network infrastructure reduced substantially. From then on, the commands that subscribers could send were limited to tone or pulse dialing of digits for signaling, switch hook flashes for simple features like call waiting and 3-way calling, and some dial access codes for features like caller-id blocking. On the subsequent incidents, never was the telephony core infrastructure compromised. The telephony operating environment, however, is experiencing dramatic changes. Companies previously labeled as telephone operators are now offering broadband data access and numerous IP services, including mail and web hosting. Furthermore, these services may not remain totally separate from the traditional telephony channels, as more closely new integrated services are offered:

- Third generation cellular phones offer voice and high-speed data communications.
- Location services enable applications to query the precise location of cellular. Phones for emergency response or targeted information/advertisement purposes.
- Many of the data-oriented applications being deployed are directly derived from Popular Internet applications, or give direct access to Internet-located information Content. The result is the current move toward all-IP and IP-interoperable networks (Figure 3). The resulting communication infrastructure, integrating voice, data and multimedia, can be considered as a part of the single large global network, the Internet. It contains traditional wired and wireless phones and computers, and increasingly multi-functional small computers presented as telephony enabled personal digital assistants (PDA). The stateless phone of yesterday is replaced by a small computer, which is both vulnerable to attacks and capable of launching attacks. With the Internet, the explosion of the communication network brought a new field of possible threats [SANS2001, CERT2001]: attacks on or through the communication infrastructure between the server and the clients. The challenge is to have a network offering the flexibility associated with the Internet, while preserving the security and reliability expected from carrier grade equipment (see figure 2.3).

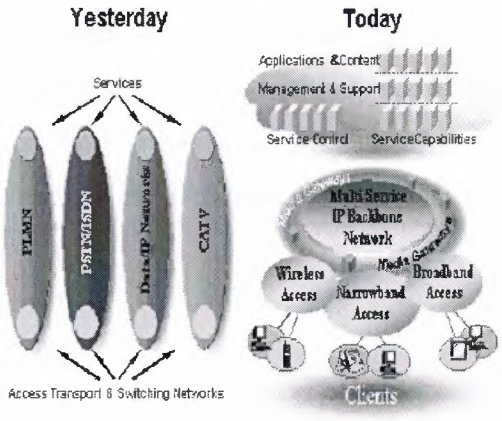

Figure 2.3 in the next generation telecom systems, the situation changes From vertical markets to an all-IP network with multiple service providers.

In security, there is the notion of an enemy that perpetrates systematic attacks against a System. Defending against systematic attacks contrasts with defending against Undesirable events that occur at random. This is a fundamental change from the Traditional telecom approach concentrated around countering undesirable events, rather Than systematic, deliberate and repetitive attacks from different sources. Defending Against random events can be accomplished by using techniques, e.g., redundancy, that Tilt the odds in one's favor. Redundancy is useless against a systematic attack since it just adds the requirement that the very same attack be performed twice or more times defending against systematic attacks requires using specific countermeasures that make Things impossible or at least very impractical for attackers.

2.6 Security Threats

An attack is an attempt to circumvent the security policy of a system, to make it do something it is not intended to do. When a possible attack is considered in context, it Becomes a threat and can be assigned a risk factor (i.e., a probability of occurrence or an Expectation of damage) that essentially serves to prioritize this type of attack. This Context includes the known or estimated vulnerabilities that are present on a system and The measures that are put in place to counter their exploitation by specific attacks. Threats Against a system are enumerated in a threat model that is the basis for developing a customized security policy, or strategy. One actual instance of an attack is referred to as An incident. Since a system can be compromised with just one breach, easiest attacks (the weakest links of the chain) must be the first ones to be countered.

2.6.1 Threat Model

For every threat, can be defined:

- Vulnerability exploited
- Countermeasures
- Likelihood

- Harm: it explains the type of the damage to the system, for example the loss of Hard Disk content
- Impact: it describes the seriousness of the attack, major or minor damages,
- Risk: it is a function of the likelihood of a threat, the resulting impact, and the Effectiveness of countermeasures to it. The table below presents the risk level According to the likelihood of a threat and its impact.

2.6.2 Types of Attacks

It is possible to classify attacks according to different factors. For example:

- Based on the techniques that are used and the vulnerabilities that are exploited
- By the kind of gain they give the attacker upon success relative to the position Held By the attacker prior to the attack.
- Remote and local attacks can be stringed together in a process known as privilege Escalation.
- Preliminary attacks can assist a main attack, e.g., by making sure The attacker remains unidentified.
- Based on the fact that origin of the attack is in internal to the corporate network or External to it. In the context of a telecom infrastructure, the possibility of local attacks must especially not be neglected. Indeed, their local systems are not limited to single switch and may be quite large and complex; they are typically clusters of resources that are connected by internal protocols. They also provide access to different users and processes with Different needs that should translate into different privileges. If we classify possible types of attacks in terms of what are
- the attackers' motivations, we can list the following attacks
- Denial of service: bringing computing or networking resources to exhaustion so That A service is unavailable, as long as the attack lasts, or the host or network Element crashes (until manual intervention or automatic re-initialization).
- Theft of service: obtaining a service for which one does not subscribe, or a better Grade of service (e.g., gold instead of silver grade QoS in DiffServ) than the one Paid
- Information theft: Unauthorized copying of information. This is typically done for

Information that can be used for financial gain (such as credit-card numbers), but Can be done for other purposes, such as software piracy.

- "Socially motivated" attacks: an attacker may wish to impersonate somebody Specific In order to commit detectable crimes and have the other person charged. Attackers may also wish to target individuals or organizations as a matter of Personal revenge, or as part of a violent activist or terrorist activity. These attacks can be performed using different mechanisms:
- Social engineering: fooling someone, with minimal or no use of technology.
- Masquerading (or impersonation): breaching authentication (which can be based On Secrets, tokens, or biometrics), for instance by theft or eavesdropping.
- Exploit of implementation flaw: purposely stimulating a system that fails t properly Validates or manipulates external inputs of all kinds in a wrong way. This Covers memory overflows, format string vulnerabilities, and improper decoding of URL % syntax and UTF-8.
- Data driven attacks: using Trojans and viruses.
- Network infrastructure attacks: exploiting design flaws in the protocols that Implement the Internet infrastructure, for example: DNS spoofing, source routing, Routing table's manipulations, Generation of many ICMP replies by sending an ICMP request to a broadcast address, TCP connections termination or hijacking, and using FTP to order one server to inject data on a specific port of another server.

2.7 Network Security Design

Because security has to be an integral part of the system from the start, and cannot be "bolted on" afterwards, it is crucial to get the security design right from the very Beginning. The security policy states the rules, responsibilities and procedures to follow to protect the network and its carried information. The network design should also apply best common practice for telecom network security. Two main inputs in the designing of network security are a threat/risk assessment and the development of a security policy. The main inputs to a threat/risk assessment are the overall security goals and security budget to ensure the planned level of security is reached the network is divided into zones with

clearly defined traffic flows encryption/VPNTechnologies are applied where necessary. It is crucial to develop a Network Plan for Security, comprising a report describing the procedures used, threats mitigated and scalability/functionality paths to follow in future phases of the development of the network. Also shown in the Network Plan are the locations of perimeter protection nodes, placement of IDS/IPS sensors, firewalls, and encryption nodes. Guideline scripts for filtering/security configuration are also produced, along with inputs to the node-hardening process. As with all security configurations, the three aspects of functionality ease of use, and security level must be carefully balanced in the design.

2.7.1 Network Configuration / Integration

When an end-to-end security architecture network configuration is carefully planned, Integration of a new network or an upgrade/enhancement of an existing network can Be performed in the best way, helping to guarantee that the planned security levels Will be implemented in a structured way.

2.7.2 Network Security Audits

Network Security audits can be performed on two levels:

- Network Security Assessment
- Network Security Analysis

Security Assessment – Network-common items such as Security Policies and Security Design, or functionality areas such as GPRS, O&M, and billing, are audited on a higher level. Documentation and plans should be studied and compared with Industry practice so that, together with interviews with key personnel, Recommendations can be produced. Security Analysis – Functionality areas or specific nodes are examined in detailed way. Node configuration scripts are checked. Log analysis, vulnerability scanning and non-destructive penetration can also be performed.

2.7.3 Network Security Implementation

The suggested security improvements from any previous security-related service Must be carefully analyzed in order to choose which ones to implement. Suggestions

Can be procedural, physical, technical or relate to the personnel

2.8 Strategic Security Management

To ensure that Communications and Network Security strategies are driven and aligned with broader organizational strategies and ensure Communications and Network Security is integrated with the other security functional disciplines.

- Definition of Communications and Network Security
- Analysis of the Organization's business security requirements, including Responsibilities for compliance
- Analysis of Network Security Requirements (department input)
- Development of Strategic Policies and the conduct of Strategic Planning to Encompass the following:
    - Roles and responsibilities
    - Communications Acceptable Use
    - Network Security pre-implementation:

- Communication encryption
- Network Security posture, including policies and goals
- Firewall policies (not rule sets)
- Network Security Review
    - Network Security post-implementation:
- Network Audit/Surveillance
- Vulnerability surveillance & technology reviews
    - Breach
- Breach of Policy and response
- Breach of Network Security and response

2.8.1 Key Processes covered in the Module

- Establish organization goals (in terms of policy setting)

2.8.2 Assumed Knowledge/Assumptions Made

- Detailed knowledge of Communication and Network theory

2.8.3 Preparatory Information

The following is a list which might be used by the practitioner in preparation for general Strategic Security Management processes:

- Analysis of Organization's business security needs, department needs
- Information from network security stakeholders
- Advice on legal compliance of acceptable network use, company direction
- Information from Organizational Best Practice

2.8.4 Organizational Implementations

The following is a list which might be used by the practitioner in implementing general Strategic Security Management processes:

- Organizational Communications Acceptable Use policy
- Organizational Communications Encryption policy
- Organizational Firewall Policy
- Organizational Network Security Review policy (for regular reviews)
- Organizational Network Audit & Surveillance policy
-Organizational Vulnerability/Technology Surveillance policy
- Organizational Breach of Policy response plan
- Organizational Break of Network Security response plan

2.9 Compliance

2.9.1 Module Objective

To ensure the Communications and Network Security program complies with standards, Legislation and best practice, both internal to the organization, as well as national and International standards and legislation N.B. Regionalized versions of ISSPCS will include analysis of national and local Legislation, standards and cultural issues. They also include

some industry specific Information. Unless a document is available for your specific region, your examination will not contain regionalized content. If a region specific document is available, then the Local examinations will be regionalized

2.9.2 Key Topics Covered in the Module

- Identify impact of relevant:
  - International legislation
  - National legislation
  - State/provincial legislation
  - Local legislation
- Identify impact of relevant:
  - International standards and guidelines
  - National standards and guidelines
  - Industry standards and guidelines
- Ensure compliance with standards and legislation, and ongoing compliance checks

2.9.3 Key Processes Covered in the Module

- Identify how international, national, state/provincial and local legislation impacts On the organization.
  - Identify how international, national, state/provincial and local standards and Guidelines impact on the organization.
  - Formulate advice for management on acceptable network use
- Identify areas of non-compliance within the organization from the compliance Survey

2.9.4 Assumed Knowledge/Assumptions Made

None

.

2.9.5 Preparatory Information

The following is a list which might be used by the practitioner in preparation for general Compliance Processes:

- International, national, state/provincial and local legislation.
- International, national and industry standards and guidelines.
- Advice on legalities of acceptable network use
- Survey of current compliance within the organization

2.9.6 Organizational Implementations

The following is a list which might be used by the practitioner in implementing general Compliance Processes:

- Information on required organizational compliance for international, national, State/provincial and local legislation
- Information on required organizational compliance for international, national, State/provincial and local standards and guidelines
- Report on Acceptable Network use agreement
- Report on non-compliance within the organization for legislation and standards

2.10 Asset Identification Classification & Valuation

2.10.1 Module Objective

To identify Communications and Network protection requirements and priorities Communications and Network security effort through assessment of asset's value.

2.10.2 Key Topics Covered In The Module

- Asset Fundamentals
-Value of Procedures and documentation
- Auditing
- Change Control
- Information/Data Protection:
    - Identification of information/data requiring protection
    - Appropriate controls/protection thereof

2.10.3 Key Processes Covered In The Module

- Collection of information on what is deemed valuable for the Organization in terms of:
  - Physical (hardware) assets
  - IP assets
  - Document assets
  - Data assets
  - Other assets (investments, software, etc)
- Asset audit, assessing (based on procedure to identify/classify/value assets):
  - Physical (hardware) assets
  - IP assets
  - Document assets
  - Data assets
- Other assets (investments, software, etc) Identification of suitable change Methods for business processes that require change
- Assess request, conferring against Change Control procedures
- Assets to be decommissioned examined for presence of value (actual asset, data Contained on asset, IP, etc). If found, asset of value to be removed if appropriate

2.10.4 Assumed Knowledge/Assumptions Made

None

2.10.5 Preparatory Information

The following is a list which might be used by the practitioner in preparation for general Asset Identification, Classification, and Valuation Processes:

- Direction for management identifying organization's values for Communications/networks assets

-Existing company communications/networks assets including:

- Physical (hardware) assets
- IP assets
- Document assets

- Data assets
- Other assets (investments, software, etc)

- Communications/networks business processes which require change/updating
- Official request for change control
- Communications/networks asset identified to be decommissioned

2.10.6 Organizational Implementations

The following is a list which might be used by the practitioner in implementing general Asset Identification, Classification, and Valuation Processes:

-Procedures to Identify, Classify and Value organizational network/communications Assets (Audit)
- List of identified organization communications/networks Assets
- Communications/networks Change Control Procedures/Reviewed Change Control Procedures
- Change request approved or rejected
- Decommissioned communications/networks asset of no value to organist

2.11 Security Risk Analysis And Assessment

2.11.1 Module Objective

To identify, analyze and assess Communications and Network Security Risks to the Organization through the application of systematic analysis and assessment Methodologies and tools.

2.11.2 Key Topics Covered In The Module

- Identify Communications and Network Security Risks:
  - Asset and its associated vulnerabilities Vulnerability analysis
  - Threat analysis
- Analyze Communications and Network Security Risks:
  - likelihood
  - Consequence

- Existing controls

- Assess and Priorities Communications and Network Security Risks

2.11.3 Key Processes Covered In The Module

- Identify Communications and Network Security Risks.
- Conduct Vulnerability analysis in relation to Communications and Network Security Issue.
- Conduct Threat analysis in relation to Communications and Network Security Issues.
- Analyze Communications and Network Security Risks
- Assess the likelihood of Communications and Network Security Risks
- Assess the consequence of Communications and Network Security Risks
- Assess the adequacy of existing control mechanisms in relation to the identified Communications and Network Security Risks
- Assess and Priorities each of the identified Communications and Network Security risks

2.11.4 Assumed Knowledge/Assumptions Made

General understanding of Risk Management concepts.

2.11.5 Preparatory Information

The following is a list which might be used by the practitioner in preparation for general Security Risk Analysis and Assessment Processes:

- Actual risks to the organization

-Existing Communications and Network Security Risk Assessments, including threat And vulnerability assessments.

2.11.6 Organizational Implementations

The following is a list which might be used by the practitioner in implementing general Security Risk Analysis Processes:

- Communications and Network Risk Assessment
- Threat and Vulnerability Assessments

2.12 Summary

In this chapter, we explained what causes problems in telecom networks? , Structured approaches to security, Managing Security, Telephony security networks, Security Threats, Network Security Design, Strategic Security Management, Compliance, Asset Identification Classification & Valuation and Security Risk Analysis & Assessment.

3. INTERNET SECURITY

3.1 overview

As of 1996, the Internet connected an estimated 13 million computers in 195 countries on every continent, even Antarctica (1). The Internet is not a single network, but a worldwide collection of loosely connected networks that are accessible by individual computer hosts in a variety of ways; including gateways, routers, dial-up connections, and Internet service providers. The Internet is easily accessible to anyone with a computer and a network connection. Individuals and organizations worldwide can reach any point on the network without regard to national or geographic boundaries or time of day.

However, along with the convenience and easy access to information come new risks. Among them are the risks that valuable information will be lost, stolen, corrupted, or misused and that the computer systems will be corrupted. If information is recorded electronically and is available on networked computers, it is more vulnerable than if the same information is printed on paper and locked in a file cabinet. Intruders do not need to enter an office or home, and may not even be in the same country. They can steal or tamper with information without touching a piece of paper or a photocopier. They can create new electronic files, run their own programs, and hide evidence of their unauthorized activity.

3.2 Basic Security Concepts

Three basic security concepts important to information on the Internet are confidentiality, integrity, and availability. Concepts relating to the people who use that information are authentication, authorization, and non repudiation.

When information is read or copied by someone not authorized to do so, the result is known as loss of confidentiality. For some types of information, confidentiality is a very important attribute. Examples include research data, medical and insurance records, new product specifications, and corporate investment strategies. In some locations, there may be a legal obligation to protect the privacy of individuals. This is particularly true for banks and loan companies; debt collectors; businesses that extend credit to their customers or issue credit

NEAR EAST UVIVERSITY

Faculty of Engineering

Department of Electrical and Electronics Engineering

NETWORK SECURITY

Graduation Project
EE- 400

Student: Ayman Abu-Khurma (20034232)

Supervisor: Dr.Jamal Abu-Husna

Nicosia-2008

ACKNOWLEDGEMENT

First of all, I would like to thanks Allah {God} for guiding me through my study.

I feel proud to pay my special regards to my project advisor ".Dr. jamal abu-Husna". He gave me too much information and did his best of efforts to make me able to complete my project. He has special respect and Devine place in my hearts.

More over I want to pay special regards to my family. They encouraged me in crises. I shall never forget their sacrifices for my education so i can start my successful life and enjoy it as they are expecting. I am nothing without their prayers.

I want to honor all those persons who have supported and helped me in my project and send to them the best of regards and acknowledge. Also my special thanks to all my friends who gave me their precious time to complete my project. Also my especial thanks go to my friends, Omer Touqan, yahea daban, zeyad Al-kayaly Mohammad al-smadi, Abedalazeez Al-natsheh, Marwan Shraideh, Haidar Al-agha, Mohammad sabri, Mohammad Al-sheab, zaqaria Abu-khurma and all the other friends.

At the end I am again thankful to all persons who helped and encouraged me to complete my project, and complete the first step of my future life.

CONTENTS

ABSTRACT

The aim of this project makes security to network in order to prevent any risk through that network & communication to accomplish successful work.

Security controls and safeguards must be implemented to reduce such risks this should take place in all levels of the network and all stages of network Development The network should be designed with security in mind and be easy to Manage. The network should be safeguarded against current vulnerabilities and regularly tested for new Vulnerabilities and threats. Risks should be mitigated and attacks logged so as to provide forensic evidence.

Introduction

The requirements of information security have undergone three major changes in the last decades the first major change was the introduction of the computer the need for protecting files and information became evident. Collection of tools designed to protect data and to avoid hacker attacks has the generic name computer security. The second major change was the introduction of distributed systems, networks and communication facilities for data communication. Network security measures are needed to protect Data during transmission. The third change is the current, rapid development of wireless networks and mobile communications. Wireless security is therefore of high priority today.

1. NETWORK

1.1 Introduction

Communication may be broadly defined as the transfer of information from one point to another. When the information is to be conveyed over any distance a communication system is usually required. Within a communication system the information transfer is frequently achieved by superimposing or modulating the information on to an electromagnetic wave which acts as a carrier for the information signal. This modulated carrier is then transmitted to the required destination where it is received and the original information signal is obtained by demodulation. Sophisticated technique have been developed for this process using electromagnetic carrier waves operating at radio frequencies as well as microwave and millimeter wave frequencies. However, communication may also be achieved using an electromagnetic carrier which is selected from the optical range of frequencies.

1.2 Historical Development

The use or visible optical carrier wave or light for communication has been common for many years. Simple systems such as signal fires, reflecting mirrors and more recently. Signalling lamps have provided successful if limited, information transfer. Moreover, as early as 1880 Alexander Graham bell reported the transmission of speech using a light beam. The photo phone proposed by Bell just four years after the invention of the telephone modulated sunlight with a diaphragm giving speech transmission over a distance of 200m However although some investigation of optical communication continued in the early part of the twentieth century its use was limited to mobile, low capacity communication links This was due to both the lack of suitable light sources and the problem that light transmission in the atmosphere is restricted to line of sight and is severely affected by disturbances such as rain, snow, fog dust and atmospheric turbulence Nevertheless, tower frequency and hence longer wavelength electromagnetic waves (i.e. radio and microwave) proved suitable carriers for information transfer in the atmosphere, being far less affected by these atmospheric conditions Depending on their wavelengths these electromagnetic carriers can be transmitted over considerable distances but are limited in the amount of information they can convey by their frequencies (i.e. the

information-carrying capacity is directly related to the bandwidth or frequency extent of the modulated carrier which is generally limited to a fixed fraction of the carrier frequency).In theory, the greater the carrier frequency, the larger the available transmission bandwidth and thus the information-carrying capacity of the communication system. For this reason radio communication was a developed to higher frequency (i.e. VHF and UHF) leading to the introduction of the even higher frequency microwave and, latterly, millimetre wave transmission. The relative frequencies and wavelengths of these types of electromagnetic wave can be observed from the electromagnetic spectrum In this context it also be noted that communication at optical frequencies offers an increase in the potential usable bandwidth by a factor of around 10^4 over high frequency microwave transmission. An additional benefit of the use of. high carrier frequencies is the general ability of the communication system to communication system to concentrate the available power within the transmitted electromagnetic wave, thus giving an improved system performance. a renewed interest in optical communication was stimulated in the early 1960s with the invention of the laser his device provided a powerful coherent light source together with the possibility of modulation at high frequency In addition, the low beam divergence of the laser made enhanced free space optical transmission a practical possibility. However, the previously mentioned constraints of light transmission in the atmosphere tended to restrict these systems to short distance applications. Nevertheless, despite the problems some modest free space optical communication links have been implemented for applications such as the linking of a television camera to a base vehicle and for data links of a few hundred meters between buildings There is also some interest in optical communication between satellites in outer space using similar techniques Although the use of the laser for free space optical communication proved some what limited, the invention of the laser instigated a tremendous research effort into the study of optical components to achieve reliable information transfer using a light wave carrier The proposals for optical communication via dielectric waveguide or optical fibres fabricated from glass to avoid degradation of the optical signal by the atmosphere were made almost simultaneously in 1966 by Kao, Hockham, and Werts Such systems were viewed as a replacement for coaxial cable or carrier transmission systems. Initially the optical fibres exhibited very high attenuation (i.e. 1000dB/ km) and were therefore not comparable with the coaxial cables they were to replace (i.e. 5 to 10dB/ km).There were also serious problems involved in jointing the fiber cables in a satisfactory manner to achieve low loss and to enable the

process to be performed relatively easily and repeatedly in the field. Nevertheless within the space of ten years optical fiber losses were reduced to below 5 db/ km and suitable low loss jointing techniques were perfected.In parallel with the development of the fiber waveguide attention was also focused on the other optical components which would constitute the optical fiber communication system. Since optical frequencies are accompanied by extremely small wavelengths the development of all these optical components essentially required a new technology. Thus semiconductor optical sources (i.e. injection lasers and light emitting diodes) and detectors (i.e. photodiodes and to a certain extent phototransistors) compatible in size with optical fibers were designed and fabricated to enable successful implementation of the optical fiber system. Initially the semiconductor lasers exhibited very short lifetimes or at best a few' hours. but significant advances in the device structure enabled lifetime greater than 1000 hr I and 7000 hr to be obtained by 1973 and 1977 respectively. These devices were originally fabricated from alloys of gallium arsenide (AlGaAs) which emitted in the near infrared between 0.8 and 0.9μ m.To obtain both the low loss and low dispersion at the same operating wavelength, new advanced single-mode fiber structures have been realized: namely, dispersion shifted and dispersion flattened fibers. Hence developments in fiber technology have continued rapidly over recent years, encompassing other specialist fiber types such a polarization maintaining fibers, as well as glass materials for even longer wavelength operation in the mid-infrared (2 to 5μm) and far-infrared (8 to 12μm) regions. In addition, the implementation of associated fiber components (splices, connector's couplers, etc) and Active optoelectronic devices (sources, detectors, amplifiers, etc.) have also moved forward with such speed that optical fiber communication technology would seem to have reached a stage of maturity within its development path Therefore high-performance reliable optical fiber communication systems are now widely deployed both within telecommunications networks and many other more localized communication application areas.

1.3 Research on the Communication Process

Much of the research on the communication process in work settings has focused on factors that can increase or decrease its effectiveness. Among the factors that can affect the flow of communication from sender to receiver are source factors, channel factors and audience factors.

1.3.1 Source Factors

These are the characteristics of the sender. One such factor is status. Generally, the higher the organizational status of the sender, the more likely the communication will be listened to and acted upon, another source factor is credibility. If the source is trusted, it is more likely that the message will receive attention a final factor is the encoding skill of the sender. These skills include the ability to speak and write clearly and to select the appropriate channel for transmitting the information.

1.3.2 Channel Factors

These are the characteristics of the vehicle of transmission of a message that affect communication. Selection of the proper channel can have an important effect on the accurate flow of communication; the channel selected can also affect the impact of the message for example, face-to-face reprimand from a supervisor might carry more weight than the same reprimand conveyed over the telephone, whenever possible, using multiple channels to present complicated information will increase the likelihood that it will be attended to and retained Semantic problems are common channel factors that can lead to a breakdown in communication. These problems may arise because different people may interpret the meanings of words differently. Semantic problems may arise because of the use of technical language or jargon, the special language that develops within a specific work environment. Jargon is typically filled with abbreviated words, acronyms and slang while jargon serves the purpose of speeding up communication between those who speak the language, it can create problems when the receiver is not "fluent" in its use. The use of jargon can also present problems when a team of workers is from different professional disciplines, all of which may use different jargon. The choice of channel can affect important work-related outcomes like job-satisfaction. Muchinsky (1977) conducted a survey using questionnaires in a number of workplaces in America and found that the frequency of face-to-face communication between supervisors and subordinates was positively related to the workers' job satisfaction, while the frequently written communications was negatively correlated with satisfaction.

1.3.3 Audience Factors

These are elements related to the receiver, such as the attention span and perceptual abilities, For example. It is essential that training information is presented at a level that matches the audience's ability to understand it. Moreover, it may be critical to consider the attention span of the target audience All-day training sessions may be appropriate for management trainees who are used to long sessions, but the attention of assembly-line workers may be lost after an hour because of their unfamiliarity with the format. The relationship to the sender may also affect the communication process. For example if the receiver is subordinate to the sender, the message may be better attended to because people are supposed to listen to their bosses. Finally, decoding skills may influence the effectiveness of communication. Research has shown that effective managers have good decoding skills in listening and responding to the needs and concerns of their subordinates. In fact, because most of the communication in work settings involves spoken communications, oral decoding skills, often referred to as listening skills, are considered to be the most effective decoding skills of all

1.4 Communication Networks and Cycles

1.4.1 The Flow of Communication In Organizations

Messages flow through communication lines and networks, giving life to the work of organizations. The communication flow in work organizations is usually classified into three types: it can flow downward through the organizational hierarchy; upward, through the same chain of command; or it can flow laterally from colleague to colleague.

1.4.2 Downward Communication

This consists of messages sent from superiors to subordinates.

Most commonly they are:

1. Instructions or directions concerning job-performance
2. Information about organizational procedures and policies
3. Feedback to the subordinates concerning job performance
4. Information to assist in the co-ordination of work tasks.

While much formal communication in organizations is downward, research indicates that most organizations still do not have enough of this communication. A number of studies

indicate that workers would like more information from their superiors about work procedures and about what is happening elsewhere in the organization. It also appears that certain types of downward communication may be particularly limited, such as feedback concerning work performance. This is especially true in companies that fail to conduct regular performance appraisals.

1.4.3 Upward Communication

This is the flow of messages from the lower levels of the organization to the upper levels It most typically consists of information managers need to perform their jobs, such as feedback concerning the status of lower-level operations, which could include reports of production output or information about any problems. The upward flow of information is critical for managers, who must use this information to make important work-related decisions. Upward communication can also involve complaints and suggestions for improvement from lower-level workers and is significant because it gives subordinates some input into the functioning of the Organization.

1.4.4 Lateral Communication

This is the flow of communication between people who are on the same level in an organization, and is particularly important when co-workers must co-ordinates their activities in order to accomplish a goal. Lateral communication can also occur between two or more departments in an organization e.g. between the production and quality-control departments. Lateral communication allows for the sharing of news and information and helps develop interpersonal relationships. But too much socializing on the job can detract from effective job performance.

1.5 Communication Network

When we look beyond two-person communication to the linkages among work groups departmental or organizational members, we are concerned with communication networks which are systems of communication lines linking various senders and receivers. The flow of information is regulated by several factors: the proximity of workers to one another, the rules governing who communicates with whom, the status hierarchy, and other elements such as job assignments and duties. Communication networks are formal and follow the organigram within an organization. Five major types have been studied in depth.

Centralized networks (Chain, Y, and Wheel) where the flow is centralized or directed through specific members. Decentralized networks, (Circle, All-Channel) where the communication flow can originate at any point and does not have to be directed through certain central group members. Centralized networks are governed by members' status within the organization; decentralized networks typically are not. Often, decentralized networks are controlled by factors such as proximity, personal preference.

1.5.1 Centralized Networks

The first centralized network – the chain – represents a five-member status hierarchy a message originates at the top or bottom of the chain and works its way upward or downward. The flow of information in a chain system is relatively slow process, but it is direct with all members in the hierarchy being made aware of the message since it must pass through each link. A related communication network is the Y (or inverted Y). It is also a hierarchical network and represents four levels of status within the organization, but its last level of communication involves more than one person. Both chain and Y are similar in speed of communication and formality of who communicates with whom The wheel network involves two status levels: a higher status member (usually a work supervisor) and four lower-lever members. The higher status member is the centre or hub through which all messages must pass. There is no direct communication between lower-level members. An example might be a sales manager and his four salespersons in the field.

1.5.2 Decentralized Networks

The circle network represents communication between members who are immediately accessible to each other, such as workers positioned side by side on an assembly line. Because messages can originate anywhere and no rules govern the direction in which messages can be sent, it can be difficult to trace the original source of a message. It has a fairly quick rate of transmission. An all-channel network allows complete freedom among communication links. Any member can freely communicate with any other member and all members are accessible to each other. Communication can be very rapid and there is maximum opportunity for feedback Boards of directors, problem-solving task forces and employees working as a team is examples of this form of communication.

1.5.3 Research

There has been extensive research on communication networks; most of it has been conducted in laboratory settings the results of these studies indicate that each of the different networks has different strengths and weaknesses Centralized networks are faster and make fewer errors in dealing with simple repetitive tasks than do decentralized networks. Decentralized networks, on the other hand, are better at dealing with complex tasks such as problem solving. In general, straightforward, repetitive tasks, such as assembly or manufacturing work, tend to operate well with a centralized communication network, while creative tasks, such as group working on a product advertising campaign, are best accomplished using decentralized networks One reason why centralized networks may have difficulty in solving complex problems is because of information overload on the central person. Because messages cannot be passed on intact to the various members efficiently and quickly, group performance suffers the type of network can also affect the satisfaction of network members. Because of restriction in who can initiate and who can communicate with whom, members in centralized networks have lower levels of satisfaction (Shaw, 1964). More specifically, the persons in the central position tend to have high levels of satisfaction due to their role, whereas the no central members have extremely low satisfaction some of the research has been criticized for oversimplifying the process. Evidence suggests that in the workplace, the differences in the speed and efficiency among the various networks may disappear over time as the group involved learns to adjust to the required pattern (Burgess, 1968). Because most of the research has been conducted in laboratory settings, there has been some concern about whether these studies will generalize to actual workplaces, although the findings do allow us to model (although simplistically) the communication networks in work organizations.

1.6 Formal and Informal Lines of Communication

1.6.1 The Hierarchy versus The Grapevine

In looking at communication networks we have considered formal lines of communication However, while every organization possesses formal lines of communication each also has informal lines known as the grapevine The grapevine can follow any course through a network and because much of the information flow in an organization is informal the

organizational grapevine is an important element of study for psychologists While formal lines of communication follow the company's organizational chart; informal lines of communication are illustrated by a sociogram,these represent other organizational members with whom members typically interact.Baird (1977) suggests that three factors typically determine the pattern of communication links that form a grapevine: friendship, usage and efficiency We pass information to our friends, we communicate with those we like and avoid communicating with those we don't like. Friendship is perhaps the most important factor that holds the grapevine together. Workers who come into contact with each other for job-related reasons are more likely to start sharing information informally (smoking rooms or areas may be an interesting source of research). Finally, the grapevine sometimes develops because it is easier and more efficient for workers to follow their own informal networks rather than formal lines of communication. In addition to being a substitute network for formal lines of communication; the grapevine also serves a vital function in maintaining social relationships among workers. Formal lines of communication tend to be task-related; the grapevine serves to meet the social needs of workers-long deemed to be important to workers. The grapevine can serve to bring workers together and encourage them to develop a sense of unity and commitment to the workgroup and organization. This can play big role in reducing absenteeism and turnover rates (Baird, 1977). The grapevine also serves to reiterate important messages sent through formal lines of communication. While the grapevine serves many important functions it can also be perceived as having a somewhat negative function: the transmission of rumours.

1.6.2 Rumours

These involve information which is presented as fact, but which may actually be true or false. Rumours are based on such things as employee expectations or wishful thinking. Many managers are concerned about the grapevine and attempt to stifle it, because they believe it to be a source of rumours which may damage the company. However, research indicates that this is a myth. The transmission of false rumours via the grapevine is actually relatively rare, and estimates indicate that the grapevine is accurate over 80% of the time. This compares well with the accuracy of messages sent over formal communication lines!

1.7 Improving Communication Flow

Increasing upward flow in organizations: Several strategies that can increase upward Communication:

- Employee Suggestion Schemes: There are a variety of ways in which workers can submit ideas usually ideas are encouraged by some sort of incentive or bonus scheme based on the amount of savings the suggestion produces. This can lead to innovations but a drawback is that the suggestion system may be used to voice complaints about conditions management is unable to change
- Grievance Systems: These are designed to change existing negative situations and must be handled delicately to protect the employee from retribution Company officials must acknowledge the receipt of the grievance to keep the channels of communication open and make it clear what action has been taken.
- Open-Door Policies: This involves setting aside times when employees can go directly to managers to discuss whatever is on their minds this bypasses the intermediate steps in the upward organizational chain ensuring important messages do indeed get to the top intact. An obvious drawback is the danger of using manager's time on what may be a trivial matter.
- Employee Surveys: This is a quick way to measure employee attitudes in order to target problem areas or to solicit ideas for improvement. Because they have the benefit of anonymity, workers can respond honestly without fear of reprisal. Feedback from management is essential to give the respondents the impression that it was not a waste of time.

1.8 The Stages of Communication Flow

1.8.1 Source

As the source of the message, you need to be clear about why you're communicating, and what you want to communicate. You also need to be confident that the information you're communicating is useful and accurate.

1.8.2 Encoding

Senders need to pay attention to the choice of an appropriate channel and avoid the use of jargon.

1.8.3 Transmission

Changes in the sense of a message may occur during transmission through information being omitted, distorted or filtered out. What gets maintained are the important or outstanding features? If messages are incomplete, people will fill in any missing parts with what appears to rationalise the message. Hence, improvements to communication include dealing with any factors that produce loss of clarity such as noise, haste, over-reliance on memory. Complex messages delivered orally need to be followed up with written material. (See figure 1.1 and 1.2 stage of communication).

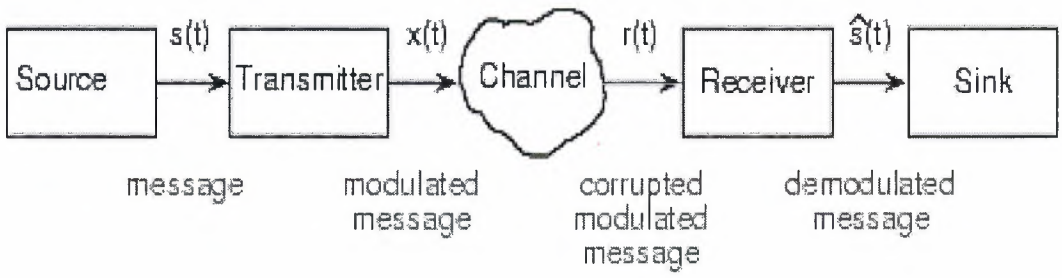

Figure 1.1 Structure of Communication System

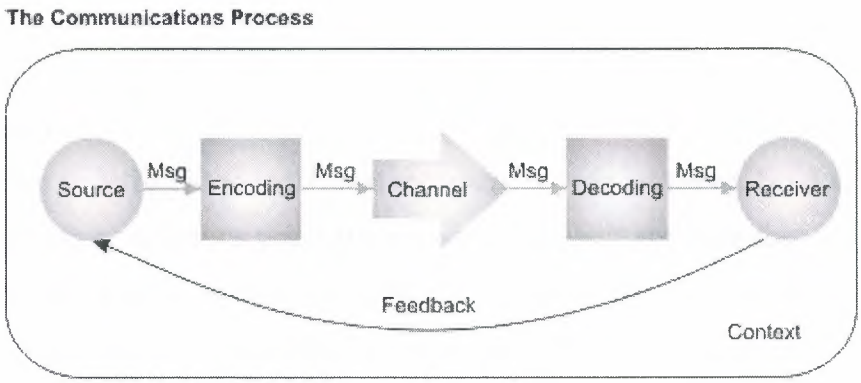

Figure 1.2 Communication Process

1.8.4 Reception

The state and context of the receiver is all important in the efficient reception of a message. Effective communication will take account of this factor.

1.8.5 Decoding

Receivers' expectations can seriously distort the content of any message they decode. People rely on their schemas when decoding information. Hence, information needs to be put into a clear context before moving onto detail

1.8.6 Feedback

Feedback is essential for effective communication to have taken place in face-to-face contact, this is immediate, but with written communication, replies (which may be tedious) are essential for the communication process to have been effectively completed.

1.8.7 Message

The message is the information that you want to communicate.

1.8.8 Channel

Messages are conveyed through channels, with verbal including face-to-face meetings, telephone and videoconferencing; and written including letters, emails, memos and reports, Different channels have different strengths and weaknesses For example, it's not particularly effective to give a long list of directions verbally, while you'll quickly cause problems if you criticize someone strongly by email.

1.8.9 Receiver

Your message is delivered to individual members of your audience. No doubt, you have in mind the actions or reactions you hope your message will get from this audience. Keep in mind, though, that each of these individuals enters into the communication process with ideas and feelings that will undoubtedly influence their understanding of your message, and their response. To be a successful communicator, you should consider these before delivering your message, and act appropriately.

1.9 Summary

In this chapter, we explained research on communication process, communication network and cycle, communication network, Formal and Informal Lines of Communication, Improving Communication Flow, and The Stages of Communication Flow.

2. NETWORK SECURITY

2.1 Introduction

As new end-user services are introduced in today's converged multi-service networks telecom network security becomes more of an issue for operators and demand from public users, enterprises and government agencies. If not given the appropriate attention, the technologies that deliver these services may actually degrade the security of the network over which the service is delivered. Security breaches, whether they disrupt services or compromise information, cause financial losses. Examples are financial penalties for failing to maintain performance agreements, lost revenue caused by network disruptions, lost consumer loyalty, ill will, lawsuits, and industrial espionage. Moreover, individual public users, agencies and corporations are demanding highly secure connections to telecom networks; service providers with roaming agreements want secure interfaces with their roaming partners and insurance providers, always conscious of risk, are insisting upon stringent security. Telecom Network Security Awareness and acting proactively can, apart from reducing risk, also reduce Operational cost. The operator needs a trustworthy security story if they are to be taken seriously in the marketplace. The Ericsson approach is to address security at an early stage in a structured Manner; from procedural, personnel, physical and technical points of view. In this Way a secure, cost Effective security solution can be established and maintained to protect sensitive information and network operator business.

2.2 What Causes Problems In Telecom Networks?

Traditionally, telecom networks refer to the infrastructure required to establish an End-to-end transfer of analogue or digital information. This comprised the transmission and switching infrastructure. Today, the infrastructure is divided into layers in order to achieve higher level of service integration. The new infrastructure supports fixed and wireless network services. Telecom networks distinguish between traffic (e.g., voice, data and multimedia) and control (signaling). A different layer, called connectivity network, is

defined for traffic, and another layer, called control layer, is defined for signaling. As more applications and services appeared, another layer was introduced, the service layer. Operations& Maintenance (O&M) networks require high security, and that leads to another sub layer within the core network. With all the advantages that we can mention about the integrated layered architecture of telecom networks, we should not overlook the increasing number of security concerns that apply to all types of services and all levels of the telecom network access networks are subject to denial-of-service attacks and various unauthorized-access attacks. Fixed networks suffer from clip-on access and associated fraud, as well as violation of privacy. Wireless networks do not require physical access, and are even more exposed. Mobility adds other vulnerabilities and threats, including SIM card cloning, subscription frauds and man-in-the-middle attacks and so on Core networks have a multitude of interconnection points, which mean different security requirements and possible exposure to a wide range of threats and vulnerabilities Attacks on the core would lead to larger impacts on the different services and stakeholders, such as end users, service and application providers, and the operator itself Stealing passwords and accessing the management ports, attacking the signaling layer, targeting databases of subscribers, HLRs, OSSs network elements, gateways, and application servers could lead to security Violations, fraud and service interruption As networks grow and become increasingly complex, the risk of holes in security due to configuration and/or design mistakes increases. As increasingly more business critical applications rely on the availability of the networks, the exposure to loss is also becoming drastically higher. Users expect reliability in all transactions, independent of access, and guaranteed connection quality. From a security point of view, the user expects no viruses, no worms, no fraud, nobody listening in, and the ability to know who requests a communication session.

2.3 Structured Approaches To Security

2.3.1 Identifying Needed Security Services And Functions

Security solution development begins with threat-risk analysis. It is required to identify assets, threats and vulnerabilities; rank the different assets in the order of their importance for the business, and evaluate different alternatives to handle the Risk.

The risks are then grouped into categories such as:

- Must be minimized/eliminated
- Should be minimized/eliminated
- Acceptable.

This information enables decision-makers to capture requirements and to specify the Implementation of security services and functions.

2.3.2 Security Policy

A security policy should be a statement of management intent, supporting the goals and principles of information security in line with the business strategy and objectives. The policy performs several functions that help ensure the effectiveness of whatever security strategy the organization pursues. Specifically, it:

- Defines information security and its overall objectives an scope.
- Defines acceptable security practices; a framework for setting control objectives. And controls, including the structure of risk assessment and risk management
- Establishes roles and responsibilities definition of general and specific responsibilities for information-security management including reporting information security incidents.

Briefly explains the security policies, principles, standards, and compliance requirements of particular importance to the organization, including:

- Compliance with legislative, regulatory, and contractual requirements
- Security education, training, and awareness requirements
- Business continuity management. The security policy framework should be the "Hub" around which all security-related services and functions evolve.

2.3.3 Network Security Architecture Reference Model

To provide adequate security, it is important to be able to model the mobile network and analyze the threats to assets. The following three-plane architecture (based on the international standard X.805) provides a useful and simple way of capturing relevant information. This model consists of four architectural components: separate security planes, security layers, security services, and security policies & principles (see figure 2.1).

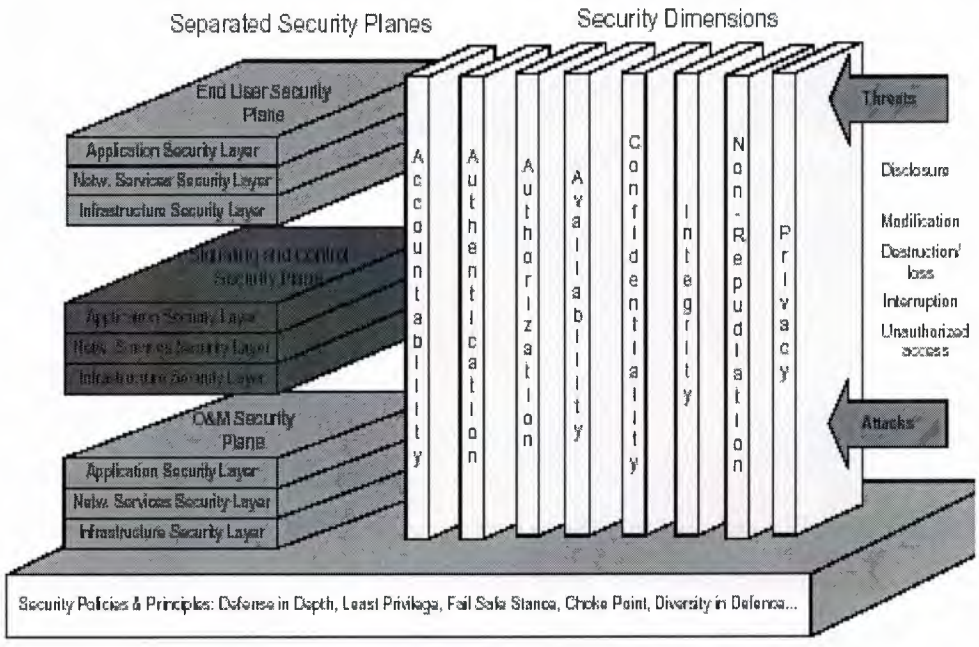

Figure 2.1 Network Security Architecture Model

2.3.4 Security Planes

Networks should be designed in such a way that events on one security plane are kept totally isolated from the other security planes. The concept of security planes provides the ability to differentiate and address security concerns independently. The End-User Security Plane addresses security of access and use of the service provider's network by customers. This plane also represents actual end-user data flows. The Signaling and Control Security Plane covers protection of the activities that enables the efficient delivery of information,

services and applications across the network. The O&M Security Plane covers the protection of operation and maintenance functions.

2.3.5 Security Dimensions

The security dimensions are system aspects which run through all security solutions. However, security solutions and mechanisms are used for implementing the security dimensions. All security dimensions should be evaluated in each security plane/layer intersection point. The most common ones are:

- Authentication
- Authorization
- Accountability
- Availability
- Confidentiality
- Integrity
- Non-repudiation and privacy

2.3.6 Security Policies And Principles

To enhance protection of the network, specific security principles and best practices are commonly used. Probably the most important one is the defense-in-depth principle: employ several security mechanisms and security layers to provide protection. If one of the mechanisms or layers fails, the other mechanisms and layers are still in place to provide sufficient protection. This principle is commonly used to protect the perimeter of a site, as depicted earlier in (Figure 2.1) the least privilege is another fundamental security principle. It means that an entity should only have the privileges it needs to perform its tasks. This is of utmost importance when considering node protection. The services running on a node should have only the privileges they need to provide the service and the node should not be running any unnecessary services. Systems and nodes should also implement the fail-safe principle. This means that when the system or node fails, it should fail without harmful side effects. Sometimes, the diversity-of-defense principle might also be useful. This principle is based on using different types of systems to provide a certain kind of protection. If one of the systems contains vulnerability, the other systems might not have that vulnerability

and the impact of the vulnerability is thus mitigated. A choke point forces attackers to use a narrow channel, which can be monitored and controlled. In network security the proper perimeter protection for the site is such a choke point; anyone attacking the site from the outside will have to go through that channel, which should be defended against such attacks.

2.4 Managing Security

To be able to make sound security judgments, both the particular business context and the networking environment must be fully understood. To support the whole telecom system life cycle, from end-to-end, the following operations have to be undertaken:

- Business Continuity Management
- Network Security Design
- Network Configuration / Integration
- Network Security Audits
- Network Security Implementation
- Fraud Management.

2.4.1 Common Principles

The security operations address

- Risk Management: all network operation implies a certain risk that must be accepted avoided, reduced or transferred.
- Business Continuity: the operator's critical processes and information should be protected from disclosure and/or disruption.
- Lowering operator costs: well thought-out security solutions provide a payback in terms of reduced operating costs, reduced risk of fraud, a reduced risk of critical security-related network outages and potentially less churn. The following chapter describes how the different sub-operations complement each other and fit into the "Security Wheel" concept, forming continuous security management.

2.4.2 The Security Wheel

This industry-standard model has been chosen to illustrate where security Management fits in, and how all security activities in a network must evolve around the security policy; the concept sees network security as a continuing process built around a

Corporate security policy. This process is divided into the stages:

- Implement network security
- Monitor network and respond to incidents
- Test the security of the network
- Improve network security. Implement network security –Security devices such as Perimeter nodes, VPN devices, firewalls, Intrusion Detection/Prevention Systems (IDS/IPS) and authentication devices are planned; configured and integrated the purpose is to prevent activities that the policy has defined as threats. Monitor/Respond the implemented security policy is validated using intrusion Detection, as well as log and other auditing techniques, to watch for violations Test the effectiveness of the policy should be evaluated at regular intervals through security audits, vulnerability scanning and/or penetration tests. Manage/Improve

Information gathered from previous steps is analyzed (see figure 2.2) and used Together with developments in the security market to improve the policy, moving around the circle to the first step again.

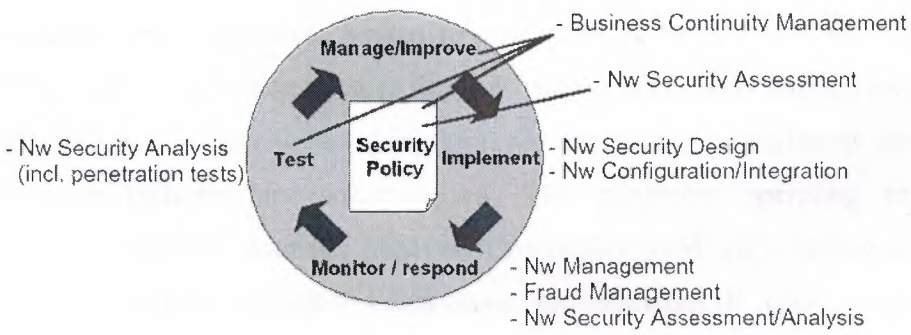

Figure 2.2 The Security Wheel model

2.4.3 Security – A continuous Process

Security Policy – Is, together with the Risk Analysis, the most fundamental part of any company's security/business continuity process. These can be checked and/or developed as a part of either the security assessment service or the business continuity service. Business Continuity also includes such aspects as, for example, crisis management, disaster recovery, and organization resiliency. Risk Analysis and Readiness planning is of utmost importance in guaranteeing the safe launch of a new service. Implement Network Security – Network Security Design ensures that security is implemented according to best telecom practices, and the level planned for in the Security policy. Also, configuration and integration must be performed in the most secure manner possible, and according to plans. Monitor/Respond – Network Management personnel monitor logs, while Intrusion Detection System real-time alarms detect any signs of attempted policy violations. Fraud-management processes and solutions instantly detect malicious end-user behavior. The network security organization must be continuously updated with the latest methodology to perform IDS/IPS tuning, log analysis and computer forensics.

2.5 Telephony Security Networks

Telephony networks typically interface to subscribers through a shallow and well-defined Interface. After the introduction of out-of-band control technology based on Signaling Contact person. System 7 (SS7) in 1970s, the number of security incidents involving the core telephone network infrastructure reduced substantially. From then on, the commands that subscribers could send were limited to tone or pulse dialing of digits for signaling, switch hook flashes for simple features like call waiting and 3-way calling, and some dial access codes for features like caller-id blocking. On the subsequent incidents, never was the telephony core infrastructure compromised. The telephony operating environment, however, is experiencing dramatic changes. Companies previously labeled as telephone operators are now offering broadband data access and numerous IP services, including mail and web hosting. Furthermore, these services may not remain totally separate from the traditional telephony channels, as more closely new integrated services are offered:

- Third generation cellular phones offer voice and high-speed data communications.
- Location services enable applications to query the precise location of cellular. Phones for emergency response or targeted information/advertisement purposes.
- Many of the data-oriented applications being deployed are directly derived from Popular Internet applications, or give direct access to Internet-located information Content. The result is the current move toward all-IP and IP-interoperable networks (Figure 3). The resulting communication infrastructure, integrating voice, data and multimedia, can be considered as a part of the single large global network, the Internet. It contains traditional wired and wireless phones and computers, and increasingly multi-functional small computers presented as telephony enabled personal digital assistants (PDA). The stateless phone of yesterday is replaced by a small computer, which is both vulnerable to attacks and capable of launching attacks. With the Internet, the explosion of the communication network brought a new field of possible threats [SANS2001, CERT2001]: attacks on or through the communication infrastructure between the server and the clients. The challenge is to have a network offering the flexibility associated with the Internet, while preserving the security and reliability expected from carrier grade equipment (see figure 2.3).

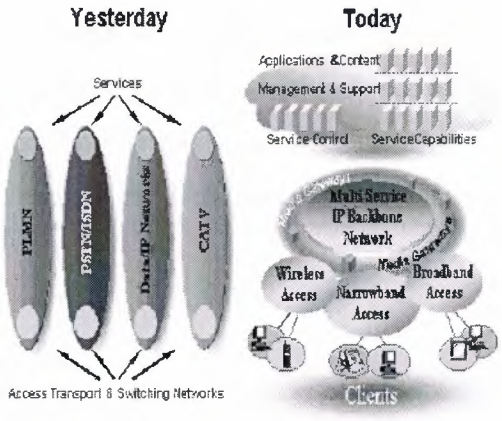

Figure 2.3 in the next generation telecom systems, the situation changes From vertical markets to an all-IP network with multiple service providers.

In security, there is the notion of an enemy that perpetrates systematic attacks against a System. Defending against systematic attacks contrasts with defending against Undesirable events that occur at random. This is a fundamental change from the Traditional telecom approach concentrated around countering undesirable events, rather Than systematic, deliberate and repetitive attacks from different sources. Defending Against random events can be accomplished by using techniques, e.g., redundancy, that Tilt the odds in one's favor. Redundancy is useless against a systematic attack since it just adds the requirement that the very same attack be performed twice or more times defending against systematic attacks requires using specific countermeasures that make Things impossible or at least very impractical for attackers.

2.6 Security Threats

An attack is an attempt to circumvent the security policy of a system, to make it do something it is not intended to do. When a possible attack is considered in context, it Becomes a threat and can be assigned a risk factor (i.e., a probability of occurrence or an Expectation of damage) that essentially serves to prioritize this type of attack. This Context includes the known or estimated vulnerabilities that are present on a system and The measures that are put in place to counter their exploitation by specific attacks. Threats Against a system are enumerated in a threat model that is the basis for developing a customized security policy, or strategy. One actual instance of an attack is referred to as An incident. Since a system can be compromised with just one breach, easiest attacks (the weakest links of the chain) must be the first ones to be countered.

2.6.1 Threat Model

For every threat, can be defined:

- Vulnerability exploited
- Countermeasures
- Likelihood

- Harm: it explains the type of the damage to the system, for example the loss of Hard Disk content
- Impact: it describes the seriousness of the attack, major or minor damages,
- Risk: it is a function of the likelihood of a threat, the resulting impact, and the Effectiveness of countermeasures to it. The table below presents the risk level According to the likelihood of a threat and its impact.

2.6.2 Types of Attacks

It is possible to classify attacks according to different factors. For example:

- Based on the techniques that are used and the vulnerabilities that are exploited
- By the kind of gain they give the attacker upon success relative to the position Held By the attacker prior to the attack.
- Remote and local attacks can be stringed together in a process known as privilege Escalation.
- Preliminary attacks can assist a main attack, e.g., by making sure The attacker remains unidentified.
- Based on the fact that origin of the attack is in internal to the corporate network or External to it. In the context of a telecom infrastructure, the possibility of local attacks must especially not be neglected. Indeed, their local systems are not limited to single switch and may be quite large and complex; they are typically clusters of resources that are connected by internal protocols. They also provide access to different users and processes with Different needs that should translate into different privileges. If we classify possible types of attacks in terms of what are
- the attackers' motivations, we can list the following attacks
- Denial of service: bringing computing or networking resources to exhaustion so That A service is unavailable, as long as the attack lasts, or the host or network Element crashes (until manual intervention or automatic re-initialization).
- Theft of service: obtaining a service for which one does not subscribe, or a better Grade of service (e.g., gold instead of silver grade QoS in DiffServ) than the one Paid
- Information theft: Unauthorized copying of information. This is typically done for

Information that can be used for financial gain (such as credit-card numbers), but Can be done for other purposes, such as software piracy.

- "Socially motivated" attacks: an attacker may wish to impersonate somebody Specific In order to commit detectable crimes and have the other person charged. Attackers may also wish to target individuals or organizations as a matter of Personal revenge, or as part of a violent activist or terrorist activity. These attacks can be performed using different mechanisms:
- Social engineering: fooling someone, with minimal or no use of technology.
- Masquerading (or impersonation): breaching authentication (which can be based On Secrets, tokens, or biometrics), for instance by theft or eavesdropping.
- Exploit of implementation flaw: purposely stimulating a system that fails t properly Validates or manipulates external inputs of all kinds in a wrong way. This Covers memory overflows, format string vulnerabilities, and improper decoding of URL % syntax and UTF-8.
- Data driven attacks: using Trojans and viruses.
- Network infrastructure attacks: exploiting design flaws in the protocols that Implement the Internet infrastructure, for example: DNS spoofing, source routing, Routing table's manipulations, Generation of many ICMP replies by sending an ICMP request to a broadcast address, TCP connections termination or hijacking, and using FTP to order one server to inject data on a specific port of another server.

2.7 Network Security Design

Because security has to be an integral part of the system from the start, and cannot be "bolted on" afterwards, it is crucial to get the security design right from the very Beginning. The security policy states the rules, responsibilities and procedures to follow to protect the network and its carried information. The network design should also apply best common practice for telecom network security. Two main inputs in the designing of network security are a threat/risk assessment and the development of a security policy. The main inputs to a threat/risk assessment are the overall security goals and security budget to ensure the planned level of security is reached the network is divided into zones with

clearly defined traffic flows encryption/VPNTechnologies are applied where necessary. It is crucial to develop a Network Plan for Security, comprising a report describing the procedures used, threats mitigated and scalability/functionality paths to follow in future phases of the development of the network. Also shown in the Network Plan are the locations of perimeter protection nodes, placement of IDS/IPS sensors, firewalls, and encryption nodes. Guideline scripts for filtering/security configuration are also produced, along with inputs to the node-hardening process. As with all security configurations, the three aspects of functionality ease of use, and security level must be carefully balanced in the design.

2.7.1 Network Configuration / Integration

When an end-to-end security architecture network configuration is carefully planned, Integration of a new network or an upgrade/enhancement of an existing network can Be performed in the best way, helping to guarantee that the planned security levels Will be implemented in a structured way.

2.7.2 Network Security Audits

Network Security audits can be performed on two levels:

- Network Security Assessment
- Network Security Analysis

Security Assessment – Network-common items such as Security Policies and Security Design, or functionality areas such as GPRS, O&M, and billing, are audited on a higher level. Documentation and plans should be studied and compared with Industry practice so that, together with interviews with key personnel, Recommendations can be produced. Security Analysis – Functionality areas or specific nodes are examined in detailed way. Node configuration scripts are checked. Log analysis, vulnerability scanning and non-destructive penetration can also be performed.

2.7.3 Network Security Implementation

The suggested security improvements from any previous security-related service Must be carefully analyzed in order to choose which ones to implement. Suggestions

Can be procedural, physical, technical or relate to the personnel

2.8 Strategic Security Management

To ensure that Communications and Network Security strategies are driven and aligned with broader organizational strategies and ensure Communications and Network Security is integrated with the other security functional disciplines.

- Definition of Communications and Network Security
- Analysis of the Organization's business security requirements, including Responsibilities for compliance
- Analysis of Network Security Requirements (department input)
- Development of Strategic Policies and the conduct of Strategic Planning to Encompass the following:
    - Roles and responsibilities
    - Communications Acceptable Use
    - Network Security pre-implementation:

- Communication encryption
- Network Security posture, including policies and goals
- Firewall policies (not rule sets)
- Network Security Review
    - Network Security post-implementation:
- Network Audit/Surveillance
- Vulnerability surveillance & technology reviews
    - Breach
- Breach of Policy and response
- Breach of Network Security and response

2.8.1 Key Processes covered in the Module

- Establish organization goals (in terms of policy setting)

2.8.2 Assumed Knowledge/Assumptions Made

- Detailed knowledge of Communication and Network theory

2.8.3 Preparatory Information

The following is a list which might be used by the practitioner in preparation for general Strategic Security Management processes:

- Analysis of Organization's business security needs, department needs
- Information from network security stakeholders
- Advice on legal compliance of acceptable network use, company direction
- Information from Organizational Best Practice

2.8.4 Organizational Implementations

The following is a list which might be used by the practitioner in implementing general Strategic Security Management processes:

- Organizational Communications Acceptable Use policy
- Organizational Communications Encryption policy
- Organizational Firewall Policy
- Organizational Network Security Review policy (for regular reviews)
- Organizational Network Audit & Surveillance policy
-Organizational Vulnerability/Technology Surveillance policy
- Organizational Breach of Policy response plan
- Organizational Break of Network Security response plan

2.9 Compliance

2.9.1 Module Objective

To ensure the Communications and Network Security program complies with standards, Legislation and best practice, both internal to the organization, as well as national and International standards and legislation N.B. Regionalized versions of ISSPCS will include analysis of national and local Legislation, standards and cultural issues. They also include

some industry specific Information. Unless a document is available for your specific region, your examination will not contain regionalized content. If a region specific document is available, then the Local examinations will be regionalized

2.9.2 Key Topics Covered in the Module

- Identify impact of relevant:
  - International legislation
  - National legislation
  - State/provincial legislation
  - Local legislation
- Identify impact of relevant:
  - International standards and guidelines
  - National standards and guidelines
  - Industry standards and guidelines
- Ensure compliance with standards and legislation, and ongoing compliance checks

2.9.3 Key Processes Covered in the Module

- Identify how international, national, state/provincial and local legislation impacts On the organization.
  - Identify how international, national, state/provincial and local standards and Guidelines impact on the organization.
  - Formulate advice for management on acceptable network use
- Identify areas of non-compliance within the organization from the compliance Survey

2.9.4 Assumed Knowledge/Assumptions Made

None

.

2.9.5 Preparatory Information

The following is a list which might be used by the practitioner in preparation for general Compliance Processes:

- International, national, state/provincial and local legislation.
- International, national and industry standards and guidelines.
- Advice on legalities of acceptable network use
- Survey of current compliance within the organization

2.9.6 Organizational Implementations

The following is a list which might be used by the practitioner in implementing general Compliance Processes:

- Information on required organizational compliance for international, national, State/provincial and local legislation
- Information on required organizational compliance for international, national, State/provincial and local standards and guidelines
- Report on Acceptable Network use agreement
- Report on non-compliance within the organization for legislation and standards

2.10 Asset Identification Classification & Valuation

2.10.1 Module Objective

To identify Communications and Network protection requirements and priorities Communications and Network security effort through assessment of asset's value.

2.10.2 Key Topics Covered In The Module

- Asset Fundamentals
-Value of Procedures and documentation
- Auditing
- Change Control
- Information/Data Protection:
    - Identification of information/data requiring protection
    - Appropriate controls/protection thereof

2.10.3 Key Processes Covered In The Module

- Collection of information on what is deemed valuable for the Organization in terms of:
  - Physical (hardware) assets
  - IP assets
  - Document assets
  - Data assets
  - Other assets (investments, software, etc)
- Asset audit, assessing (based on procedure to identify/classify/value assets):
  - Physical (hardware) assets
  - IP assets
  - Document assets
  - Data assets
- Other assets (investments, software, etc) Identification of suitable change Methods for business processes that require change
- Assess request, conferring against Change Control procedures
- Assets to be decommissioned examined for presence of value (actual asset, data Contained on asset, IP, etc). If found, asset of value to be removed if appropriate

2.10.4 Assumed Knowledge/Assumptions Made

None

2.10.5 Preparatory Information

The following is a list which might be used by the practitioner in preparation for general Asset Identification, Classification, and Valuation Processes:

- Direction for management identifying organization's values for Communications/networks assets

-Existing company communications/networks assets including:

- Physical (hardware) assets
- IP assets
- Document assets

- Data assets
- Other assets (investments, software, etc)

- Communications/networks business processes which require change/updating
- Official request for change control
- Communications/networks asset identified to be decommissioned

2.10.6 Organizational Implementations

The following is a list which might be used by the practitioner in implementing general Asset Identification, Classification, and Valuation Processes:

-Procedures to Identify, Classify and Value organizational network/communications Assets (Audit)
- List of identified organization communications/networks Assets
- Communications/networks Change Control Procedures/Reviewed Change Control Procedures
- Change request approved or rejected
- Decommissioned communications/networks asset of no value to organist

2.11 Security Risk Analysis And Assessment

2.11.1 Module Objective

To identify, analyze and assess Communications and Network Security Risks to the Organization through the application of systematic analysis and assessment Methodologies and tools.

2.11.2 Key Topics Covered In The Module

- Identify Communications and Network Security Risks:
  - Asset and its associated vulnerabilities Vulnerability analysis
  - Threat analysis
- Analyze Communications and Network Security Risks:
  - likelihood
  - Consequence

- Existing controls

- Assess and Priorities Communications and Network Security Risks

2.11.3 Key Processes Covered In The Module

- Identify Communications and Network Security Risks.
- Conduct Vulnerability analysis in relation to Communications and Network Security Issue.
- Conduct Threat analysis in relation to Communications and Network Security Issues.
- Analyze Communications and Network Security Risks
- Assess the likelihood of Communications and Network Security Risks
- Assess the consequence of Communications and Network Security Risks
- Assess the adequacy of existing control mechanisms in relation to the identified Communications and Network Security Risks
- Assess and Priorities each of the identified Communications and Network Security risks

2.11.4 Assumed Knowledge/Assumptions Made

General understanding of Risk Management concepts.

2.11.5 Preparatory Information

The following is a list which might be used by the practitioner in preparation for general Security Risk Analysis and Assessment Processes:

- Actual risks to the organization

-Existing Communications and Network Security Risk Assessments, including threat And vulnerability assessments.

2.11.6 Organizational Implementations

The following is a list which might be used by the practitioner in implementing general Security Risk Analysis Processes:

- Communications and Network Risk Assessment
- Threat and Vulnerability Assessments

2.12 Summary

In this chapter, we explained what causes problems in telecom networks? , Structured approaches to security, Managing Security, Telephony security networks, Security Threats, Network Security Design, Strategic Security Management, Compliance, Asset Identification Classification & Valuation and Security Risk Analysis & Assessment.

3. INTERNET SECURITY

3.1 overview

As of 1996, the Internet connected an estimated 13 million computers in 195 countries on every continent, even Antarctica (1). The Internet is not a single network, but a worldwide collection of loosely connected networks that are accessible by individual computer hosts in a variety of ways; including gateways, routers, dial-up connections, and Internet service providers. The Internet is easily accessible to anyone with a computer and a network connection. Individuals and organizations worldwide can reach any point on the network without regard to national or geographic boundaries or time of day.

However, along with the convenience and easy access to information come new risks. Among them are the risks that valuable information will be lost, stolen, corrupted, or misused and that the computer systems will be corrupted. If information is recorded electronically and is available on networked computers, it is more vulnerable than if the same information is printed on paper and locked in a file cabinet. Intruders do not need to enter an office or home, and may not even be in the same country. They can steal or tamper with information without touching a piece of paper or a photocopier. They can create new electronic files, run their own programs, and hide evidence of their unauthorized activity.

3.2 Basic Security Concepts

Three basic security concepts important to information on the Internet are confidentiality, integrity, and availability. Concepts relating to the people who use that information are authentication, authorization, and non repudiation.

When information is read or copied by someone not authorized to do so, the result is known as loss of confidentiality. For some types of information, confidentiality is a very important attribute. Examples include research data, medical and insurance records, new product specifications, and corporate investment strategies. In some locations, there may be a legal obligation to protect the privacy of individuals. This is particularly true for banks and loan companies; debt collectors; businesses that extend credit to their customers or issue credit

cards; hospitals, doctors' offices, and medical testing laboratories; individuals or agencies that offer services such as psychological counseling or drug treatment; and agencies that collect taxes.

Information can be corrupted when it is available on an insecure network. When information is modified in unexpected ways, the result is known as loss of integrity. This means that unauthorized changes are made to information, whether by human error or intentional tampering. Integrity is particularly important for critical safety and financial data used for activities such as electronic funds transfers, air traffic control, and financial accounting. Information can be erased or become inaccessible, resulting in loss of availability. This means that people who are authorized to get information cannot get what they need. Availability is often the most important attribute in service-oriented businesses that depend on information (e.g., airline schedules and online inventory systems). Availability of the network itself is important to anyone whose business or education relies on a network connection. When a user cannot get access to the network or specific services provided on the network, they experience a denial of service.

To make information available to those who need it and who can be trusted with it, organizations use authentication and authorization. Authentication is proving that a user is whom he or she claims to be. That proof may involve something the user knows (such as a password), something the user has (such as a "smartcard"), or something about the user that proves the person's identity (such as a fingerprint). Authorization is the act of determining whether a particular user (or computer system) has the right to carry out a certain activity, such as reading a file or running a program. Authentication and authorization go hand in hand. Users must be authenticated before carrying out the activity they are authorized to perform. Security is strong when the means of authentication cannot later be refuted - the user cannot later deny that he or she performed the activity. This is known as non repudiation.

3.3 Why Care About Security?

It is remarkably easy to gain unauthorized access to information in an insecure networked environment, and it is hard to catch the intruders. Even if users have nothing stored on their computer that they consider important, that computer can be a "weak link", allowing unauthorized access to the organization's systems and information. Seemingly innocuous information can expose a computer system to compromise. Information that intruders find useful includes which hardware and software are being used, system configuration, type of network connections, phone numbers, and access and authentication procedures. Security-related information can enable unauthorized individuals to get access to important files and programs, thus compromising the security of the system. Examples of important information are passwords, access control files and keys, personnel information, and encryption algorithms. The consequences of a break-in cover a broad range of possibilities: a minor loss of time in recovering from the problem, a decrease in productivity, a significant loss of money or staff-hours, a devastating loss of credibility or market opportunity, a business no longer able to compete, legal liability, and the loss of life.

3.4 Network Security Incidents

A network security incident is any network-related activity with negative security implications. This usually means that the activity violates an explicit or implicit security policy (see the section on security policy). Incidents come in all shapes and sizes. They can come from anywhere on the Internet, although some attacks must be launched from specific systems or networks and some require access to special accounts. An intrusion may be a comparatively minor event involving a single site or a major event in which tens of thousands of sites are compromised. (When reading accounts of incidents, note that different groups may use different criteria for determining the bounds of an incident.) A typical attack pattern consists of gaining access to a user's account, gaining privileged access, and using the victim's system as a launch platform for attacks on other sites. It is possible to accomplish all these steps manually in as little as 45 seconds; with automation, the time decreases further.

3.5 Sources Of Incidents

It is difficult to characterize the people who cause incidents. An intruder may be an adolescent who is curious about what he or she can do on the Internet, a college student who has created a new software tool, an individual seeking personal gain, or a paid "spy" seeking information for the economic advantage of a corporation or foreign country. An incident may also be caused by a disgruntled former employee or a consultant who gained network information while working with a company. An intruder may seek entertainment, intellectual challenge, a sense of power, political attention, or financial gain. One characteristic of the intruder community as a whole is its communication. There are electronic newsgroups and print publications on the latest intrusion techniques, as well as conferences on the topic. Intruders identify and publicize misconfigured systems; they use those systems to exchange pirated software, credit card numbers, exploitation programs, and the identity of sites that have been compromised, including account names and passwords. By sharing knowledge and easy-to-use software tools, successful intruders increase their number and their impact.

3.6 Types Of Incidents

Incidents can be broadly classified into several kinds: the probe, scan, account compromise, root compromise, packet sniffer, denial of service, exploitation of trust, malicious code, and Internet infrastructure attacks.

- **Probe**

A probe is characterized by unusual attempts to gain access to a system or to discover information about the system. One example is an attempt to log in to an unused account. Probing is the electronic equivalent of testing doorknobs to find an unlocked door for easy entry. Probes are sometimes followed by a more serious security event, but they are often the result of curiosity or confusion.

- **Scan**

A scan is simply a large number of probes done using an automated tool. Scans can sometimes be the result of a misconfiguration or other error, but they are often a prelude to a more directed attack on systems that the intruder has found to be vulnerable.

- **Account Compromise**

An account compromise is the unauthorized use of a computer account by someone other than the account owner, without involving system-level or root-level privileges (privileges a system administrator or network manager has). An account compromise might expose the victim to serious data loss, data theft, or theft of services. The lack of root-level access means that the damage can usually be contained, but a user-level account is often an entry point for greater access to the system.

- **Root Compromise**

A root compromise is similar to an account compromise, except that the account that has been compromised has special privileges on the system. The term *root* is derived from an account on UNIX systems that typically has unlimited, or "superuser", privileges. Intruders who succeed in a root compromise can do just about anything on the victim's system, including run their own programs; change how the system works, and hide traces of their intrusion.

- **Packet Sniffer**

A packet snifter is a program that captures data from information packets as they travel over the network. That data may include user names, passwords, and proprietary information that travel over the network in clear text. With perhaps hundreds or thousands of passwords captured by the sniffer, intruders can launch widespread attacks on systems. Installing a packet sniffer does not necessarily require privileged access. For most multi-user systems, however, the presence of a packet sniffer implies there has been a root compromise.

- **Denial Of Service**

The goal of denial-of-service attacks is not to gain unauthorized access to machines or data, but to prevent legitimate users of a service from using it. A denial-of-service attack can come in many forms. Attackers may "flood" a network with large volumes of data or deliberately consume a scarce or limited resource, such as process control blocks or pending network connections. They may also disrupt physical components of the network or manipulate data in transit, including encrypted data.

- **Exploitation Of Trust**

Computers on networks often have trust relationships with one another. For example, before executing some commands, the computer checks a set of files that specify which other computers on the network are permitted to use those commands. If attackers can forge their identity, appearing to be using the trusted computer, they may be able to gain unauthorized access to other computers.

- **Malicious Code**

Malicious code is a general term for programs that, when executed, would cause undesired results on a system. Users of the system usually are not aware of the program until they discover the damage. Malicious code includes Trojan horses, viruses, and worms. Trojan horses and viruses are usually hidden in legitimate programs or files that attackers have altered to do more than what is expected. Worms are self-replicating programs that spread with no human intervention after they are started. Viruses are also self-replicating programs, but usually require some action on the part of the user to spread inadvertently to other programs or systems. These sorts of programs can lead to serious data loss, downtime, denial of service, and other types of security incidents.

- **Internet Infrastructure Attacks**

These rare but serious attacks involve key components of the Internet infrastructure rather than specific systems on the Internet. Examples are network name servers, network access providers, and large archive sites on which many users depend. Widespread automated

attacks can also threaten the infrastructure. Infrastructure attacks affect a large portion of the Internet and can seriously hinder the day-to-day operation of many sites.

- **Incidents And Internet Growth**

Since the CERT® Coordination Center began operating in 1988, the number of security incidents reported to the center has grown dramatically, from less than 100 in 1988 to almost 2,500 in 1995, the last year for which complete statistics are available as of this writing. Through 1994, the increase in incident reports roughly parallels the growth of the size of the Internet during that time. Figure3.1 shows the growth of the Internet and the corresponding growth of reported security incidents.

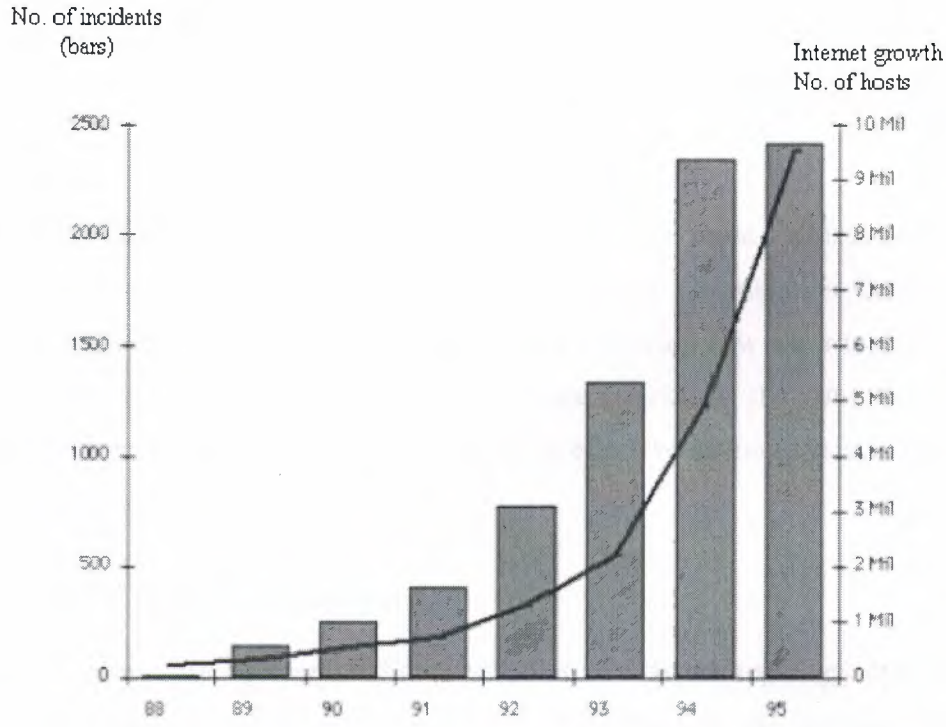

Figure 3.1 Growths in Security Incidents

The data for 1995 and partial data for 1996 show a slowing of the rate at which incidents are reported to the CERT/CC (perhaps because of sites' increased security efforts or the significant increase in other response teams formed to handle incidents). However, the rate

continues to increase for serious incidents, such as root compromises, services outages, and packet sniffers.

3.7 Incident Trends

In the late 1980s and early 1990s, the typical intrusion was fairly straightforward. Intruders most often exploited relatively simple weaknesses, such as poor passwords and misconfigured systems that allowed greater access to the system than was intended. Once on a system, the intruders exploited one or another well-known, but usually unfixed, vulnerability to gain privileged access, enabling them to use the system as they wished.

There was little need to be more sophisticated because these simple techniques were effective. Vendors delivered systems with default settings that made it easy to break into systems. Configuring systems in a secure manner was not straightforward, and many system administrators did not have the time, expertise, or tools to monitor their systems adequately for intruder activity.

Unfortunately, all these activities continue in 1996; however, more sophisticated intrusions are now common. In eight years of operation, the CERT Coordination Center has seen intruders demonstrate increased technical knowledge, develop new ways to exploit system vulnerabilities, and create software tools to automate attacks. At the same time, intruders with little technical knowledge are becoming more effective as the sophisticated intruders share their knowledge and tools.

3.8 Intruders' Technical knowledge

Intruders are demonstrating increased understanding of network topology, operations, and protocols, resulting in the infrastructure attacks described in the previous section on Internet infrastructure attacks. Instead of simply exploiting well-known vulnerabilities, intruders examine source code to discover weaknesses in certain programs, such as those used for electronic mail. Much source code is easy to obtain from programmers who make their work freely available on the Internet. Programs written for research purposes (with little thought for security) or written by naive programmers become widely used, with

source code available to all. Moreover, the targets of many computer intrusions are organizations that maintain copies of proprietary source code (often the source code to computer operating systems or key software utilities). Once intruders gain access, they can examine this code to discover weaknesses.

Intruders keep up with new technology. For example, intruders now exploit vulnerabilities associated with the World Wide Web to gain unauthorized access to systems. Other aspects of the new sophistication of intruders include the targeting of the network infrastructure (such as network routers and firewalls) and the ability to cloak their behavior. Intruders use Trojan horses to hide their activity from network administrators; for example, intruders alter authentication and logging programs so that they can log in without the activity showing up in the system logs. Intruders also encrypt output from their activity, such as the information captured by packet sniffers. Even if the victim finds the sniffer logs, it is difficult or impossible to determine what information was compromised.

3.9 Techniques To Exploit Vulnerabilities

As intruders become more sophisticated, they identify new and increasingly complex methods of attack. For example, intruders are developing sophisticated techniques to monitor the Internet for new connections. Newly connected systems are often not fully configured from a security perspective and are, therefore, vulnerable to attacks.

The most widely publicized of the newer types of intrusion is the use of the packet sniffers described in the section above on packet sniffers. Other tools are used to construct packets with forged addresses; one use of these tools is to mount a denial-of-service attack in a way that obscures the source of the attack. Intruders also "spoof" computer addresses, masking their real identity and successfully making connections that would not otherwise be permitted. In this way, they exploit trust relationships between computers.

With their sophisticated technical knowledge and understanding of the network, intruders are increasingly exploiting network interconnections. They move through the Internet infrastructure, attacking areas on which many people and systems depend. Infrastructure

attacks are even more threatening because legitimate network managers and administrators typically think about protecting systems and parts of the infrastructure rather than the infrastructure as a whole.

In the first quarter of 1996, 7.5% of 346 incidents handled by the CERT Coordination Center involved these new and sophisticated methods, including packet sniffers, spoofing, and infrastructure attacks. A full 20% involved the total compromise of systems, in which intruders gain system-level, or root, privileges. This represents a significant increase in such attacks over previous years' attacks, and the numbers are still rising. Of 341 incidents in the third quarter of 1996, nearly 9% involved sophisticated attacks, and root compromises accounted for 33%.

3.10 Intruders' Use Of Software Tools

The tools available to launch an attack have become more effective, easier to use, and more accessible to people without an in-depth knowledge of computer systems. Often a sophisticated intruder embeds an attack procedure in a program and widely distributes it to the intruder community. Thus, people who have the desire but not the technical skill are able to break into systems. Indeed, there have been instances of intruders breaking into a UNIX system using a relatively sophisticated attack and then attempting to run DOS commands (commands that apply to an entirely different operating system).

Tools are available to examine programs for vulnerabilities even in the absence of source code. Though these tools can help system administrators identify problems, they also help intruders find new ways to break into systems.

As in many areas of computing, the tools used by intruders have become more automated, allowing intruders to gather information about thousands of Internet hosts quickly and with minimum effort. These tools can scan entire networks from a remote location and identify individual hosts with specific weaknesses. Intruders may catalog the information for later exploitation, share or trade with other intruders, or attack immediately. The increased

availability and usability of scanning tools means that even technically naive, would-be intruders can find new sites and particular vulnerabilities.

Some tools automate multiphase attacks in which several small components are combined to achieve a particular end. For example, intruders can use a tool to mount a denial-of-service attack on a machine and spoof that machine's address to subvert the intended victim's machine. A second example is using a packet sniffer to get router or firewall passwords, logging in to the firewall to disable filters, then using a network file service to read data on an otherwise secure server.

The trend toward automation can be seen in the distribution of software packages containing a variety of tools to exploit vulnerabilities. These packages are often maintained by competent programmers and are distributed complete with version numbers and documentation.

A typical tool package might include the following:

- network scanner
- password cracking tool and large dictionaries
- packet sniffer
- variety of Trojan horse programs and libraries
- tools for selectively modifying system log files
- tools to conceal current activity
- tools for automatically modifying system configuration files
- tools for reporting bogus checksums

3.11 Internet Vulnerabilities

A vulnerability is a weakness that a person can exploit to accomplish something that is not authorized or intended as legitimate use of a network or system. When a vulnerability is exploited to compromise the security of systems or information on those systems, the result is a security incident. Vulnerabilities may be caused by engineering or design errors, or faulty implementation.

3.11.1 Why The Internet Is Vulnerable

Many early network protocols that now form part of the Internet infrastructure were designed without security in mind. Without a fundamentally secure infrastructure, network defense becomes more difficult. Furthermore, the Internet is an extremely dynamic environment, in terms of both topology and emerging technology.

Because of the inherent openness of the Internet and the original design of the protocols, Internet attacks in general are quick, easy, inexpensive, and may be hard to detect or trace. An attacker does not have to be physically present to carry out the attack. In fact, many attacks can be launched readily from anywhere in the world - and the location of the attacker can easily be hidden. Nor is it always necessary to "break in" to a site (gain privileges on it) to compromise confidentiality, integrity, or availability of its information or service.

Even so, many sites place unwarranted trust in the Internet. It is common for sites to be unaware of the risks or unconcerned about the amount of trust they place in the Internet. They may not be aware of what can happen to their information and systems. They may believe that their site will not be a target or that precautions they have taken are sufficient. Because the technology is constantly changing and intruders are constantly developing new tools and techniques, solutions do not remain effective indefinitely. Since much of the traffic on the Internet is not encrypted, confidentiality and integrity are difficult to achieve. This situation undermines not only applications (such as financial applications that are network-based) but also more fundamental mechanisms such as authentication and no repudiation (see the section on basic security concepts for definitions). As a result, sites may be affected by a security compromise at another site over which they have no control. An example of this is a packet sniffer that is installed at one site but allows the intruder to gather information about other domains (possibly in other countries).

Another factor that contributes to the vulnerability of the Internet is the rapid growth and use of the network, accompanied by rapid deployment of network services involving complex applications. Often, these services are not designed, configured, or maintained

securely. In the rush to get new products to market, developers do not adequately ensure that they do not repeat previous mistakes or introduce new vulnerabilities. Compounding the problem, operating system security is rarely a purchase criterion. Commercial operating system vendors often report that sales are driven by customer demand for performance, price, ease of use, maintenance, and support. As a result, off-the-shelf operating systems are shipped in an easy-to-use but insecure configuration that allows sites to use the system soon after installation. These hosts/sites are often not fully configured from a security perspective before connecting. This lack of secure configuration makes them vulnerable to attacks, which sometimes occur within minutes of connection.

Finally, the explosive growth of the Internet has expanded the need for well-trained and experienced people to engineer and manage the network in a secure manner. Because the need for network security experts far exceeds the supply, inexperienced people are called upon to secure systems, opening windows of opportunity for the intruder community.

3.11.2 Types Of Technical Vulnerabilities

The following taxonomy is useful in understanding the technical causes behind successful intrusion techniques, and helps experts identify general solutions for addressing each type of problem.

3.12 Flaws In Software Or Protocol Designs

Protocols define the rules and conventions for computers to communicate on a network. If a protocol has a fundamental design flaw, it is vulnerable to exploitation no matter how well it is implemented. An example of this is the Network File System (NFS), which allows systems to share files. This protocol does not include a provision for authentication; that is, there is no way of verifying that a person logging in really is whom he or she claims to be. NFS servers are targets for the intruder community.

When software is designed or specified, often security is left out of the initial description and is later "added on" to the system. Because the additional components were not part of

the original design, the software may not behave as planned and unexpected vulnerabilities may be present.

3.12.1 Weaknesses In How Protocols And Software Are Implemented

Even when a protocol is well designed, it can be vulnerable because of the way it is implemented. For example, a protocol for electronic mail may be implemented in a way that permits intruders to connect to the mail port of the victim's machine and fool the machine into performing a task not intended by the service. If intruders supply certain data for the "To:" field instead of a correct E-mail address, they may be able to fool the machine into sending them user and password information or granting them access to the victim's machine with privileges to read protected files or run programs on the system. This type of vulnerability enables intruders to attack the victim's machine from remote sites without access to an account on the victim's system. This type of attack often is just a first step, leading to the exploitation of flaws in system or application software.

Software may be vulnerable because of flaws that were not identified before the software was released. This type of vulnerability has a wide range of subclasses, which intruders often exploit using their own attack tools. For readers who are familiar with software design, the following examples of subclasses are included:

- race conditions in file access
- non-existent checking of data content and size
- non-existent checking for success or failure
- inability to adapt to resource exhaustion
- incomplete checking of operating environment
- inappropriate use of system calls
- re-use of software modules for purposes other than their intended ones

By exploiting program weaknesses, intruders at a remote site can gain access to a victim's system. Even if they have access to a no privileged user account on the victim's system, they can often gain additional, unauthorized privileges.

3.12.2 Weaknesses In System And Network Configuration

Vulnerabilities in the category of system and network configurations are not caused by problems inherent in protocols or software programs. Rather, the vulnerabilities are a result of the way these components are set up and used. Products may be delivered with default settings that intruders can exploit. System administrators and users may neglect to change the default settings, or they may simply set up their system to operate in a way that leaves the network vulnerable.

An example of a faulty configuration that has been exploited is anonymous File Transfer Protocol (FTP) service. Secure configuration guidelines for this service stress the need to ensure that the password file, archive tree, and ancillary software are separate from the rest of the operating system, and that the operating system cannot be reached from this staging area. When sites misconfigure their anonymous FTP archives, unauthorized users can get authentication information and use it to compromise the system.

3.13 Security Policy, Procedures, And Practices

3.13.1 Security Policy

A policy is a documented high-level plan for organization-wide computer and information security. It provides a framework for making specific decisions, such as which defense mechanisms to use and how to configure services, and is the basis for developing secure programming guidelines and procedures for users and system administrators to follow. Because a security policy is a long-term document, the contents avoid technology-specific issues. A security policy covers the following (among other topics appropriate to the organization):

- high-level description of the technical environment of the site, the legal environment (governing laws), the authority of the policy, and the basic philosophy to be used when interpreting the policy
- risk analysis that identifies the site's assets, the threats that exist against those assets, and the costs of asset loss

- guidelines for system administrators on how to manage systems
- definition of acceptable use for users
- guidelines for reacting to a site compromise (e.g., how to deal with the media and law enforcement, and whether to trace the intruder or shutdown and rebuild the system)

Factors that contribute to the success of a security policy include management commitment, technological support for enforcing the policy, effective dissemination of the policy, and the security awareness of all users. Management assigns responsibility for security, provides training for security personnel, and allocates funds to security. Technological support for the security policy moves some responsibility for enforcement from individuals to technology.

The result is an automatic and consistent enforcement of policies, such as those for access and authentication. Technical options that support policy include (but are not limited to)

- challenge/response systems for authentication
- auditing systems for accountability and event reconstruction
- encryption systems for the confidential storage and transmission of data
- network tools such as firewalls and proxy servers

3.13.2 Security-Related Procedures

Procedures are specific steps to follow that are based on the computer security policy. Procedures address such topics as retrieving programs from the network, connecting to the site's system from home or while traveling, using encryption, authentication for issuing accounts, configuration, and monitoring.

3.13.3 Security Practices

System administration practices play a key role in network security. Checklists and general advice on good security practices are readily available. Below are examples of commonly recommended practices:

- Ensure all accounts have a password and that the passwords are difficult to guess. A one-time password system is preferable.
- Use tools such as MD5 checksums (8), a strong cryptographic technique, to ensure the integrity of system software on a regular basis.
- Use secure programming techniques when writing software. These can be found at security-related sites on the World Wide Web.
- Be vigilant in network use and configuration, making changes as vulnerabilities become known.
- Regularly check with vendors for the latest available fixes and keep systems current with upgrades and patches.
- Regularly check on-line security archives, such as those maintained by incident response teams, for security alerts and technical advice.
- Audit systems and networks, and regularly check logs. Many sites that suffer computer security incidents report that insufficient audit data is collected, so detecting and tracing an intrusion is difficult.

3.13.4 Security Technology

A variety of technologies have been developed to help organizations secure their systems and information against intruders. These technologies help protect systems and information against attacks, detect unusual or suspicious activities, and respond to events that affect security. In this section, the focus is on two core areas: operational technology and cryptography. The purpose of operational technology is to maintain and defend the availability of data resources in a secure manner. The purpose of cryptography is to secure the confidentiality, integrity, and authenticity of data resources.

3.14 Operational Technology

Intruders actively seek ways to access networks and hosts. Armed with knowledge about specific vulnerabilities, social engineering techniques, and tools to automate information gathering and systems infiltration, intruders can often gain entry into systems with

disconcerting ease. System administrators face the dilemma of maximizing the availability of system services to valid users while minimizing the susceptibility of complex network infrastructures to attack. Unfortunately, services often depend on the same characteristics of systems and network protocols that make them susceptible to compromise by intruders. In response, technologies have evolved to reduce the impact of such threats. No single technology addresses all the problems. Nevertheless, organizations can significantly improve their resistance to attack by carefully preparing and strategically deploying personnel and operational technologies. Data resources and assets can be protected, suspicious activity can be detected and assessed, and appropriate responses can be made to security events as they occur.

One-Time Passwords Intruders often install packet sniffers to capture passwords as they traverse networks during remote log-in processes. Therefore, all passwords should at least be encrypted as they traverse networks. A better solution is to use one-time passwords because there are times when a password is required to initiate a connection before confidentiality can be protected.

One common example occurs in remote dial-up connections. Remote users, such as those traveling on business, dial in to their organization's modem pool to access network and data resources. To identify and authenticate themselves to the dial-up server, they must enter a user ID and password. Because this initial exchange between the user and server may be monitored by intruders, it is essential that the passwords are not reusable. In other words, intruders should not be able to gain access by masquerading as a legitimate user using a password they have captured.

One-time password technologies address this problem. Remote users carry a device synchronized with software and hardware on the dial-up server. The device displays random passwords, each of which remains in effect for a limited time period (typically 60 seconds). These passwords are never repeated and are valid only for a specific user during the period that each is displayed. In addition, users are often limited to one successful use of any given password. One-time password technologies significantly reduce unauthorized entry at gateways requiring an initial password.

Monitoring Tools Continuous monitoring of network activity is required if a site is to maintain confidence in the security of its network and data resources. Network monitors may be installed at strategic locations to collect and examine information continuously that may indicate suspicious activity. It is possible to have automatic notifications alert system administrators when the monitor detects anomalous readings, such as a burst of activity that may indicate a denial-of-service attempt. Such notifications may use a variety of channels, including electronic mail and mobile paging. Sophisticated systems capable of reacting to questionable network activity may be implemented to disconnect and block suspect connections, limit or disable affected services, isolate affected systems, and collect evidence for subsequent analysis.

Tools to scan, monitor, and eradicate viruses can identify and destroy malicious programs that may have inadvertently been transmitted onto host systems. The damage potential of viruses ranges from mere annoyance (e.g., an unexpected "Happy Holidays" jingle without further effect) to the obliteration of critical data resources. To ensure continued protection, the virus identification data on which such tools depend must be kept up to date. Most virus tool vendors provide subscription services or other distribution facilities to help customers keep up to date with the latest viral strains.

Security Analysis Tools Because of the increasing sophistication of intruder methods and the vulnerabilities present in commonly used applications, it is essential to assess periodically network susceptibility to compromise. A variety of vulnerability identification tools are available, which have garnered both praise and criticism. System administrators find these tools useful in identifying weaknesses in their systems. Critics argue that such tools, especially those freely available to the Internet community, pose a threat if acquired and misused by intruders.

3.15 Information Warfare

Extensive and widespread dependence on the Internet has called new attention to the importance of information to national security. The term information warfare refers to the act of war against the information resources of an adversary. Like warfare on land or in the

air, information warfare is one component of a range of attack strategies for dominating an adversary in order to gain or maintain an objective.

Information warfare is divided into two categories: offensive and defensive. The purpose of offensive information warfare is to attack the information resources of an adversary to gain dominance. Defensive information warfare is the protection of your information assets against attack.

Information assets can take many forms, from messages sent by courier in diplomatic bags to the computers used to analyze enemy positions based on satellite data. In computer security, information assets include digital information, the computers that process them, and the networks that transmit the digital information from place to place. Computer security is a key element for protecting the availability, integrity, and confidentiality of all these information assets.

Internet security protects information assets consisting of computers, information, and networks that are part of the Internet. Internet security is related to information warfare when the Internet contains information assets that are important to the information warfare objective. For example, if an adversary can use the Internet to access battle plans, the Internet is being used for information warfare. Internet security is important to both offensive and defensive information warfare because the Internet is a global and dependable resource on which many countries rely. Historically, military networks and computers were unreachable by nonmilitary participants. The Internet, however, provides a cost-effective way for military and government units to communicate and participate in achieving objectives. Use of the Internet means that individuals, multinational companies, and terrorist organizations all can gain access to important information resources of governments and military forces. Thus, it is important to address Internet security concerns as a key component of defensive information warfare. Because the Internet is global, it can be an avenue of attack for offensive information warfare by many governments. One of the battlefields for a future military offensive could very well involve the Internet. Intruder technology (as described in a separate section above) could be used by a government as a weapon against information resources, or used randomly by a terrorist organization against

civilian targets. In the study of information warfare, there are many new problems to solve that are not evident in other forms of warfare. These problems include identifying the enemy, responding without making your systems vulnerable to attack, and gathering intelligence on the Internet about preparations for a military exercise. These and other problems are likely to be the subject of discussion and investigation for some time to come.

3.16 Summary

In this chapter we discussed the internet security, basic security concepts, why care about security, network security incidents, sources of incidents, types of incidents, the vulnerabilities of internet, flaws in software or protocol design, security policy, procedures, practices and last the operational technology of security.

4. MOBILE INTERNET SECURITY

4.1 Internet Security Overview

For an understanding of security on the Mobile Internet, some knowledge is required of how security Works on the terrestrial Internet. This section explains the ways in which confidential information sent Across the Internet can be protected against interception, alteration and forgery by third parties.

4.2 Aspects Of Internet Security

To be considered entirely secure, any method of communication must offer the following features

- **Privacy** A message must not be readable by third parties between its source and its destination.
- **Integrity protection** A message must reach its destination in the same form as it left its source, or Else the fact that it has been altered in transit must be obvious to its recipient.
- **Authentication** Means must exist for the recipient of a message to verify that its Sender is Trustworthy and genuine (that is, not impersonating a third party)
- **Non-repudiation** The sender of a message must not be able to deny, at a later Time, having sent it. All these features are available on the Internet through the use of encryption, hashing, digital certificates, Digital signatures and password protection. These techniques are discussed in detail later in this section. Firstly, it is important to know why they are necessary to begin with.

4.3 Insecurity Of The Internet

The Internet is not an inherently secure medium. A message sent across the Internet from one computer to another typically travels via several intermediate computers, called routers. Anyone with access to a Router can inspect or modify data packets as they pass through it. Furthermore, before and after its Journey across the Internet, data will often pass through a local area network (LAN). The architecture of Most LANs is such that data packets from

and to one computer on the network can freely be read by any other computer on it. All this means that a message transmitted across the Internet can potentially be seen, and even altered, by hundreds of people (some known to the sender, others unknown) on its Way to its destination.

4.4 Secure Sockets Layer (SSL)

A solution to the problem of secure Internet communication was first developed by the software Company Netscape in 1994. Netscape added a protocol layer, the Secure Sockets Layer (SSL), On top of The Internet's TCP/IP protocol suite in its Navigator Web browser. SSL employs a collection Of Mathematical and computational techniques to allow data to be sent securely across the Internet in Ways that meets all the criteria of privacy, integrity protection, authentication and non-repudiation. By 1998, SSL was firmly integrated into the infrastructure of the Internet as a whole, and was the Main catalyst behind the e-commerce boom of the late 1990s. As Figure 4.1 shows, it can be used in conjunction with any of the higher-level Internet protocols, such as HTTP, File Transfer Protocol (FTP) and Internet Message Access Protocol (IMAP).

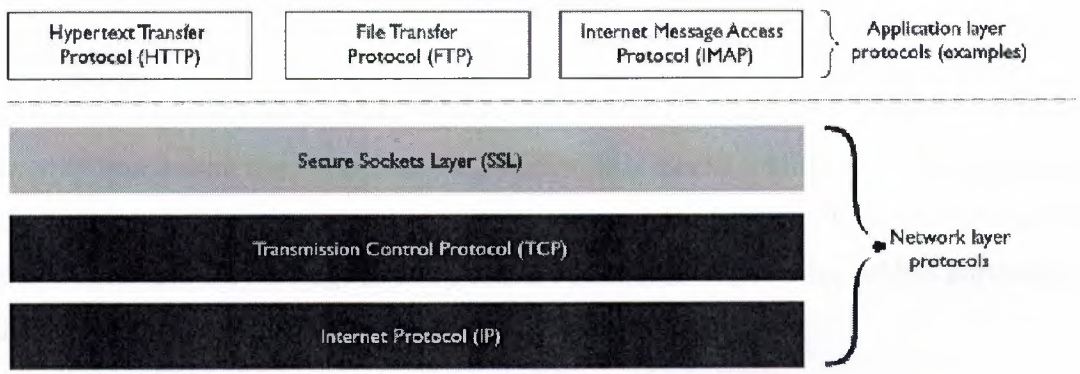

Figure 4.1 SSL's position among the Internet's protocols

SSL uses the following methods to provide security across the Internet

- **Cryptography** This is the science of scrambling messages so that they cannot easily be understood by anyone other than their sender and their intended recipient. It enables privacy in Internet Communications.
- **Message hashing** a message is run through a computational algorithm to produce a message' Fingerprint', which can be used to verify that the message has not been altered in transit.
- **Digital certificates** a digital certificate is a short electronic document that vouches for the Authenticity of its holder. It is issued by an organization called a certificate authority (CA) and is Formatted in such a way that it is practically impossible to counterfeit.
- **Digital signatures** a digital signature is a way of formatting a message so that it is Traceable to one Source and one source only. Digital signatures enable non-repudiation in Internet transactions. The methods used by SSL are generic mathematical and procedural ones, which can be applied to any secure means of communication. As we shall see in Section 3, they have already been adopted by the Mobile Internet's Wireless Transport Layer Security (WTLS) protocol and they are likely to form the basis of any future developments in Internet security.

4.5 Privacy

The fundamental requirement of any method of secure communication is privacy. In inherently transparent media such as the Internet, this means finding ways of ensuring that even if a third party can see a message, they cannot understand it. The best way to achieve this is to scramble the message in away that is systematic whilst being all but impossible to deduce from the scrambled message alone.

4.5.1 Symmetric Key Cryptography

SSL uses techniques of cryptography to scramble and unscramble data. Cryptography is the art of rendering information opaque by passing it through mathematical scrambling algorithms. The scrambling of information using cryptography is called encryption; it's unscrambling In encryption, message data Is passed through a mathematical algorithm

involving a particular numeric value. This numeric value Is called the key. In basic cryptography, a message can only easily be decrypted by someone with
Access to the key with which it was encrypted. Other important cryptographic terms are

- **Plaintext** Unencrypted data. Despite its name, the term usually refers to any kind of unencrypted data, whether textual, graphical, audio or binary.
- **Cipher text** Data that has been encrypted.
- **Cryptanalysis** The study of methods to 'break' cipher text (that is, deduce its original plaintext form) without direct access to its encryption key, encryption algorithm, or both. An example of a very Simple cryptographic algorithm is to add a value x (the key) to the code of each character in a message

- To decrypt an encrypted message, its recipient must know both its encryption algorithm and the algorithm's key. They can then use the key to perform the inverse of the encryption Operation On each character of the message. For example, if a message were encrypted by adding 6 to the Code of each character in it, it would be decrypted by subtracting 6 from each code. Because the Decryption operation is the exact inverse of the encryption operation, this type of cryptography is called Symmetric key cryptography. The algorithms that are actually used in symmetric key cryptography On the Internet are much more complex than this example, in order to be able to withstand attempts to Crack them by trial-and-error (known as 'brute force attacks').Mostsymmetricalgorithms encrypt Messages not a character at a time, but a block of bits at a time (typically 64) (a method called block cipher encryption). In block cipher Encryption, a complicated series of transformations is applied to each block in turn, using a very long key (ideally at least 112 bits). In addition, a technique called cipher block chaining is often applied, whereby the result of the encryption of each block is used as a filter for the encryption of the next block (see Figure 4.2). Cipher block chaining hides any repeated patterns of data that occur in the plaintext message. (Such patterns are always a useful 'handle' for malicious cryptanalysts.)

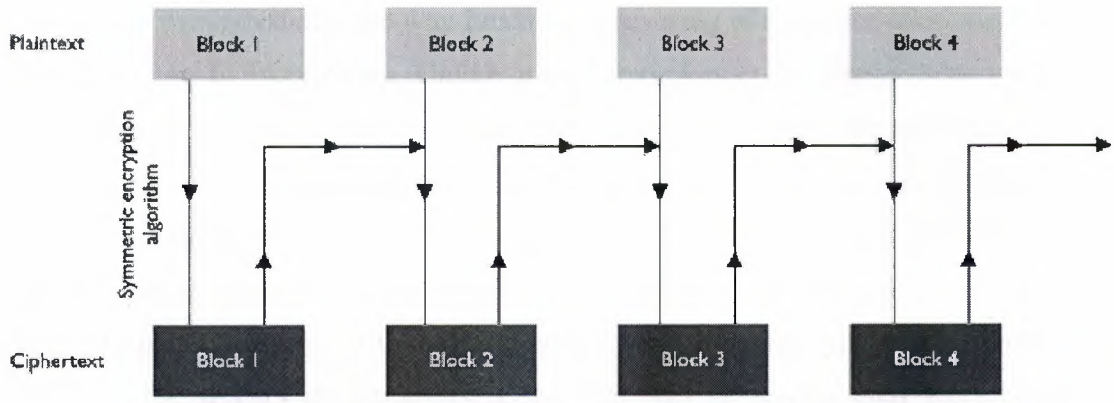

Figure 4.2 Cipher block chaining

4.5.2 Public Key Cryptography

Advanced symmetric key cryptography offers very effective security for most purposes. (According toOne estimate, there is not enough energy available in the solar system to perform a computational brute Force attack against a 256-bit key.) However, symmetric key cryptography has an important limitation before any encrypted communication can take place, the encryption key itself must be securely conveyed from the sender to the recipient. Symmetric key cryptography only allows this to be done by extraneous Means. For example, the sender could send the key in an armored van to the recipient (this is how banks Install keys in their cash machines). Of course, this undermines the main advantage of the Internet over other forms of communication, namely its practicality. To circumvent this limitation of symmetric Key cryptography, another type of cryptography, called public key cryptography (also known as asymmetric key cryptography) is employed for the exchange of symmetric keys. Public key cryptography exploits the existence of a type of mathematical operation called a one-way function. A one-way function is one that is much easier to perform in one direction than in the other. A simple example of a one-way function is the multiplication of prime numbers: for instance, it is much easier to multiply 4253 by 5521 than it is to find the two prime factors of 23480813. (The multiplication of prime numbers plays a significant role in many cryptographic algorithms.)Public key

cryptography uses advanced one-way functions, consisting of a mathematical algorithm and a Numerical key, to encrypt data. Unlike in symmetric key cryptography, however, the key used to encrypt message cannot be used to decrypt it. Decrypting the message requires a different key that is mathematically related to the encryption key, but for all practical purposes impossible to derive from it. Even knowing the encryption algorithm is no help in calculating the encryption key, for which reason the Best-known encryption algorithms are kept in the public domain. (The thinking is that submitting Encryption algorithms to the scrutiny of the world's cryptanalysts is the best way of testing their Robustness. For example, the RSA algorithm used by Alligata Secure has so far yielded no significant weaknesses.)Note that deriving a decryption key from an encryption key is always hypothetically possible; in fact, mathematically it is many times quicker to work out a private asymmetric key than it is to work out asymmetric key of the same length. Still, calculating a private asymmetric key of 1792 bits should (for the Next few years, at least) be all but computationally infeasible even using hundreds of thousands of Computers working in parallel. Certainly, for almost every organization in the world, it will be financially Infeasible.

4.5.3 Cryptography In Practice

Let us suppose Brian wants to set up a secure Internet connection. He first uses appropriate software Tool to create an asymmetric key pair, consisting of one public and one private key. Others can then use His public key to encrypt messages to him, which he (and no one else) can read using his private key in this way; anyone can send Brian a private message without going through the risk or inconvenience Of Exchanging symmetric keys beforehand. Conversely, if Brian wants to send a message that others can be sure originated with him, he encrypts it using his private key, and others use his public key to Read it. (This is the process of creating a digital Signature, and is elaborated in Section 4.8)In practice, the complex mathematical processes used by public key cryptography make it rather slow for use with Long messages. SSL therefore restricts its use of public key cryptography to the exchange of asymmetric key (see Section 4.3.) between the client and the server at the start of a secure Internet Session. This symmetric key is agreed on-the-fly between the client and the server and it is called the Session key. After the session is over,

it is discarded by both the client and the server. The ways in which symmetric and asymmetric cryptography are combined in real Internet transactions

4.6 Integrity Protection

We have seen how cryptography can be used to send messages across the Internet that is unreadable by Third parties. However, this does not prevent third parties from blindly altering messages between their Source and their destination. Depending on the content of the message, such alterations may be apparent to the recipient of the message or not. (For example, indiscriminate interference with a text message is usually easier to spot than with a block of binary data.)Integrity protection is the term applied to techniques for verifying that a message reaches its intended Recipient in exactly the same form as it leaves its sender. While integrity protection does not guarantee that a message will reach its desination unchanged, it does (virtually) guarantee that any change is Obvious to the recipient.

4.6.1 Hash Functions

Integrity protection uses computational algorithms called hash functions. A hash function is a one-way Function into which data (such as an Internet message) is fed, and whose result is value of a fixed length in bits. Passing a message through a hash function produces a hash value that ineffectively a 'fingerprint' of the message. This fingerprint is called the message digest. It is usually much Shorter than the message itself. The sender of a message computes its digest, encrypts the digest using their private key and sends it appended to the message. The recipient verifies the integrity of the message by decrypting the digest using the sender's public key, then running the message through the same hashing algorithm that produced the digest. If the message has been interfered with on its journey, the hash value calculated by the recipient will not match the value of the digest. In fact, a matching hash value is not an absolute guarantee of integrity: a collision is theoretically possible, whereby the modified message happens to produce exactly the same hash value as the original Message. However, collisions in good-quality hash functions are so rare that their calculation may be considered computationally intractable.

4.7 Authentication

SSL allows privacy and integrity in Internet communications. However, without further measures, the Anonymity of the Internet makes it easy for a user to impersonate another user. For example, a malicious Party could create a Web site on which they masquerade as a respected organization, set up a private Connection for transactions, and begin obtaining money and credit card details from unsuspecting 'Customers'.

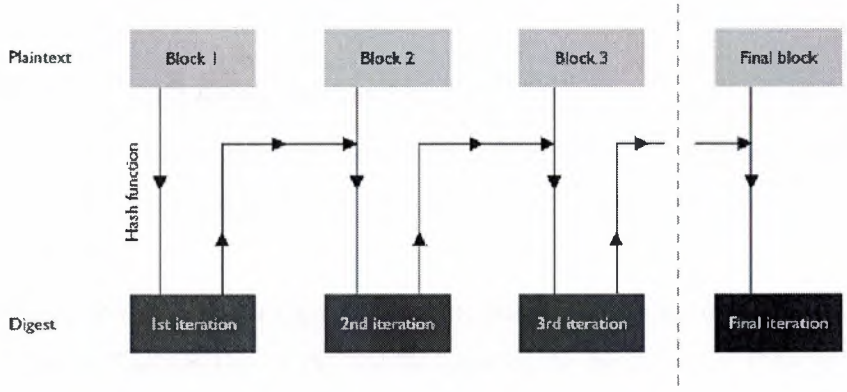

Figure 4.3 Creation of a message digests using a hash function

4.7.1 Digital Certificates

This problem is addressed by the use of digital certificates. A digital certificate is a message sent by one Party to another at the beginning of a secure Internet session, verifying the sender's identity and vouching for their integrity. The certificate is obtained from an organization called a certificate authority (CA) The certificate is virtually impossible to forge, for reasons that are explained later. Once a secure session has been requested by an Internet client such as a Web browser, it typically continues with the server sending the client its digital certificate. The server's digital certificate contains the following information

- The server's public key
- The certificate's serial number
- The certificate's validity period
- The server's domain name

- The domain name of the CA that issued the certificate

The certificate is supplied with its hashed digest (see Section 2.5.1). The digest is encrypted using the Private Key of the CA that issued the certificate; this encrypted digest constitutes the CA's digital Signature. If the digital signature can be decrypted using the CA's public key, then the certificate must have originated with the CA. (See Section 4.8 for more on digital signatures.)Upon receiving the server's certificate, the client validates it by checking the following criteria

- That it is valid for the current date.
- That it applies to the server that sent it That the CA that issued it is known and Trusted. (To do this, the client checks the CA's own certificate, which is signed by the CA itself?)
- That the CA's digital signature can be decrypted using the CA's public key. (Most Web Clients Contain list of the public keys of the best known CAs, so they do not need to search the Internet for them. The client warns the user if the certificate fails any of these tests. The user may continue with the session at their own risk, if they wish.
- Digital certificates can be issued in chains. For example, a large CA might issue a Certificate to a smaller CA, which issues a certificate to a still smaller CA, which issues end-entity certificates to Internet Traders. This helps distribute the task of administering digital certificates. When an Internet client Receives a certificate from a chain, it checks the certificate of every CA in the chain as described above, Until it reaches the self-signed certificate of a top-level CA.Digital certificates are not only used by Internet servers: they can also be obtained for Internet clients. In Practice, though, demand for client certificates has proved minimal. Authentication of a client by a server, where it is implemented at all, is usually through use of a user name and a password. While this method is not infallible, it nevertheless adds a layer of security to Internet transactions that is absent from many on
- Internet confidential transactions (for example, ordering goods by credit card over the Telephone)

4.8 Non-Repudiation

The final requirement of secure communications is non-repudiation: a message's source must be provable upon demand. Non-repudiation is normally achieved using digital signatures.

4.8.1 Digital Signatures

A digital signature is simply a way of encoding data so that its source and its integrity are verifiable Digital signatures use the same techniques of cryptography and hashing that are used to provide privacy and integrity protection (see Sections 4.4d 4.5)he difference is that the roles of public and private Keys are reversed. Let us suppose that Abigail wants to stamp a message with her digital signature. First she passes the message through a hash function to create a message digest. She then uses her private key to encrypt the digest, and attaches the encrypted digest to the message. This encrypted digest constitutes her digital signature. (Of course, Abigail could encrypt the entire message using her private key; however, encrypting the digest is sufficient and much quicker.)If Brian is the recipient of Abigail's message and wants to verify that it originated with her, he uses Abigail's public key to decrypt her signature. He then runs the message through the same hash function that Abigail used To create the digest, and compares it with the value of Abigail's decrypted signature. The main users of digital signatures on the Internet at present are CAs, who stamps them on every certificate they issue (see Section 4.7) although client-side digital signatures are an effective means of on-repudiation, demand for them has so far been minimal. This suggests that businesses and customers are happy to carry out transactions without them. Instead, client-side non-repudiation is normally implemented using password protection, which is regarded as an acceptable compromise between practicality and guaranteed security

4.9 Wireless Transport Layer Security (WTLS)

Mobile Internet security uses the same methods of encryption, hashing, digital certificates and digital Signatures that SSL provides for the terrestrial Internet. However, instead of SSL, the Mobile Internet is served by a streamlined protocol called Wireless Transport

Layer Security (WTLS).WTLS is an Optional component of the Mobile Internet's Wireless Application Protocol (WAP) stack. It resides Between the Wireless Datagram Protocol (WDP) and the Wireless Transaction Protocol (WTP) layers of The WAP stack. The structure of the WAP stack is shown in Figure 4.4

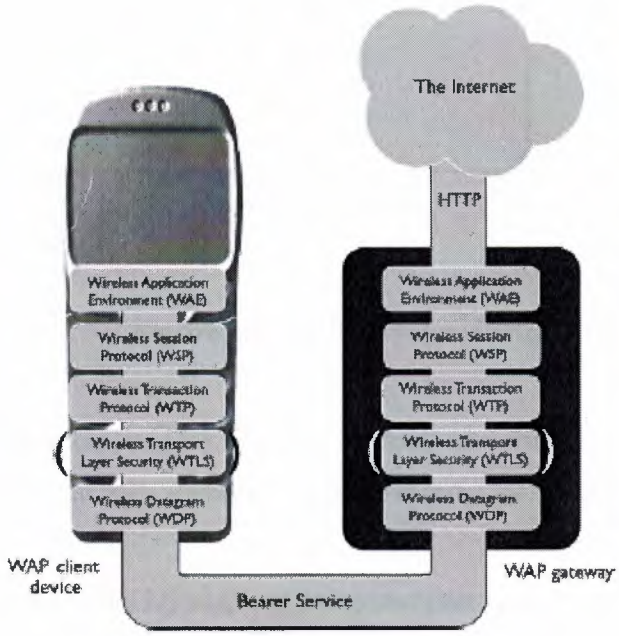

Figure 4.4 The WAP stack

Like any Mobile Internet transaction, a secure Mobile Internet transaction extends across both the mobile Telephone network and the Internet, using WAP for the wireless part of the journey, the Hypertext Transfer Protocol (HTTP) suite for the Internet part, and a WAP gateway in the middle to translate between the two. Figure 4.5 shows an overview of Mobile Internet communication, from the mobile device at one end to the HTTP server at the other. If security is required across the whole communication Channel, SSL can be used between the WAP gateway and the HTTP server. Alternatively, the content Provider can host the gateway themselves. (As will be seen later, this arrangement provides optimum Security).

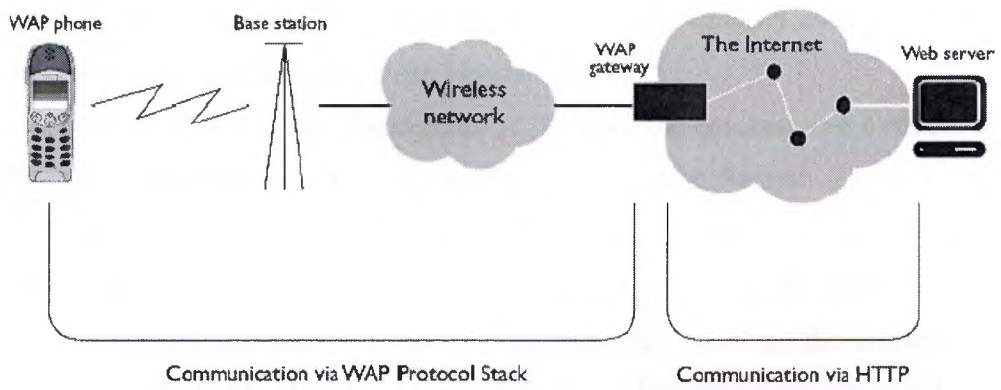

Figure 4.5 WAP communication overview

Like WAP as a whole, WTLS uses the Internet as a model for its procedures and is very similar, in Outline, to SSL. However, it has a number of additional characteristics:

- Compact coding. WTLS employs more compact coding than SSL, in order to keep Messages as short as possible and to minimize the time and processing power required by the client device to interpret and transmit them. These measures help to offset the speed limitations imposed by the high latency and low bandwidth of wireless networks. They also compensate for the low power and computational Resources of mobile devices.
- Datagram support. WTLS operates directly above WAP's Wireless Datagram Protocol (WDP), and therefore needs to accommodate the unreliability and unpredictability of connectionless datagram Communication. Rigorous confirmation and retransmission procedures are rendered doubly important by the intermittency and variable quality of radio transmission.
- Optimized handshakes. WTLS allows the WAP gateway, acting as a server to the Mobile WAP client, to authenticate the client by obtaining the client's digital certificate from an external source, rather than the client itself. This reduces the processing and memory burden on the client.

- Dynamic key refreshing. Communication via radio signals is particularly vulnerable to 'Tapping' by Third parties. As an extra security measure against eavesdropping, WTLS allows for the symmetric Session key to be changed regularly over the course of the session, without the need for a clean Handshake.
- Fast encryption and hashing algorithms. WTLS uses the quickest, most efficient Algorithms Available for hashing and encryption (see Section 2), so those clients processing time and power Consumption are kept within reasonable limits.
- Client-gateway rather than client-server coverage. Unlike SSL, WTLS does not span The whole of the communication channel from the client to the content provider's HTTP server, but only Communication over the mobile telephone network between the client and the WAP gateway. If Security is also required between the gateway and the HTTP server; it must be implemented using SSL.

4.9.1 WTLS Implementation Classes

The WTLS specification allows for three classes (levels) of WTLS implementation

- **Class 1** Anonymous encryption. Data is encrypted, but certificates are not exchanged between the Client and the gateway.
- **Class 2** Encryption with server authentication. Data is encrypted and the client requires a digital Certificate from the server.
- **Class 3** Encryption with client and server authentication. Data is encrypted and the client and the Server exchange digital certificates.

4.9.2 WTLS Handshake

The WTLS handshake is very similar to the SSL handshake. The following example illustrates the most Common form of the WTLS handshake, that for WTLS class 2 (see Section 4.9.1). This involves the Client authenticating the gateway, but not vice versa. It is illustrated in Figure 9.This example shows the full handshake. WTLS also uses an abbreviated handshake for resumption of a previously established session. This involves re-exchanging a session identification code agreed when the session was first established.

1. Bollocks!

2. Abigail, a WAP phone user, sees an item she would like to buy on a WAP site.

3. Abigail activates a link on her WAP phone that sends a request for a secure Internet session to the WAP gateway. The following information is appended to the request:

- Various information about what versions of WTLS Abigail's WAP browser supports, what Encryption algorithms it supports, and so on.
- Some randomly generated data. This will be used, along with other data, to generate the session Key (see steps 5 onward).

4. The gateway receives Abigail's request for a secure session and sends her the following Items

- Its digital certificate, including its public key. The certificate is signed by a trusted CA Using its Private Key
- Information about what versions of WTLS, encryption algorithms and so on are Supported by theWAP gateway.
- Some randomly generated data which will be used in the generation of the session key.

In WTLS class 3 (see Section 4.9.1) the gateway would also request Abigail's digital certificate at This point. Alternatively, it could obtain Abigail's certificate from an external source on the Internet -A procedure which characterizes the optimized WTLS handshake.

5. Abigail validates the gateway's certificate as outlined in Section 2.6.1. If the validation is successful, she is happy that the gateway's proprietor is genuine and trustworthy.

6. Abigail performs a series of operations on the random data she sent to the gateway, And the random data the gateway sent to her, to produce the premaster secret.

7. Abigail encrypts the premaster secret using the gateway's public key and sends it to the gateway. (InWTLS class 3; she would also send her digital certificate for the gateway to validate.)

8. The gateway receives the premaster secret from Abigail

9. The gateway decrypts the premaster secret. The gateway and Abigail simultaneously perform a Series of operations on it, to arrive at the master secret.

10. Abigail and the gateway simultaneously perform a series of operations on the master secret to arrive at the session key (see Section 4.5.3), which will be used to encrypt the information they want to Send to each other.

11. Abigail sends the gateway two messages. The first confirms that all further messages from her will be encrypted using the session key. The second is an encrypted message that formally ends the Handshake from her side.

12. The gateway sends Abigail two messages. The first confirms that all further messages from it will be encrypted using the session key. The second is an encrypted message that formally ends the

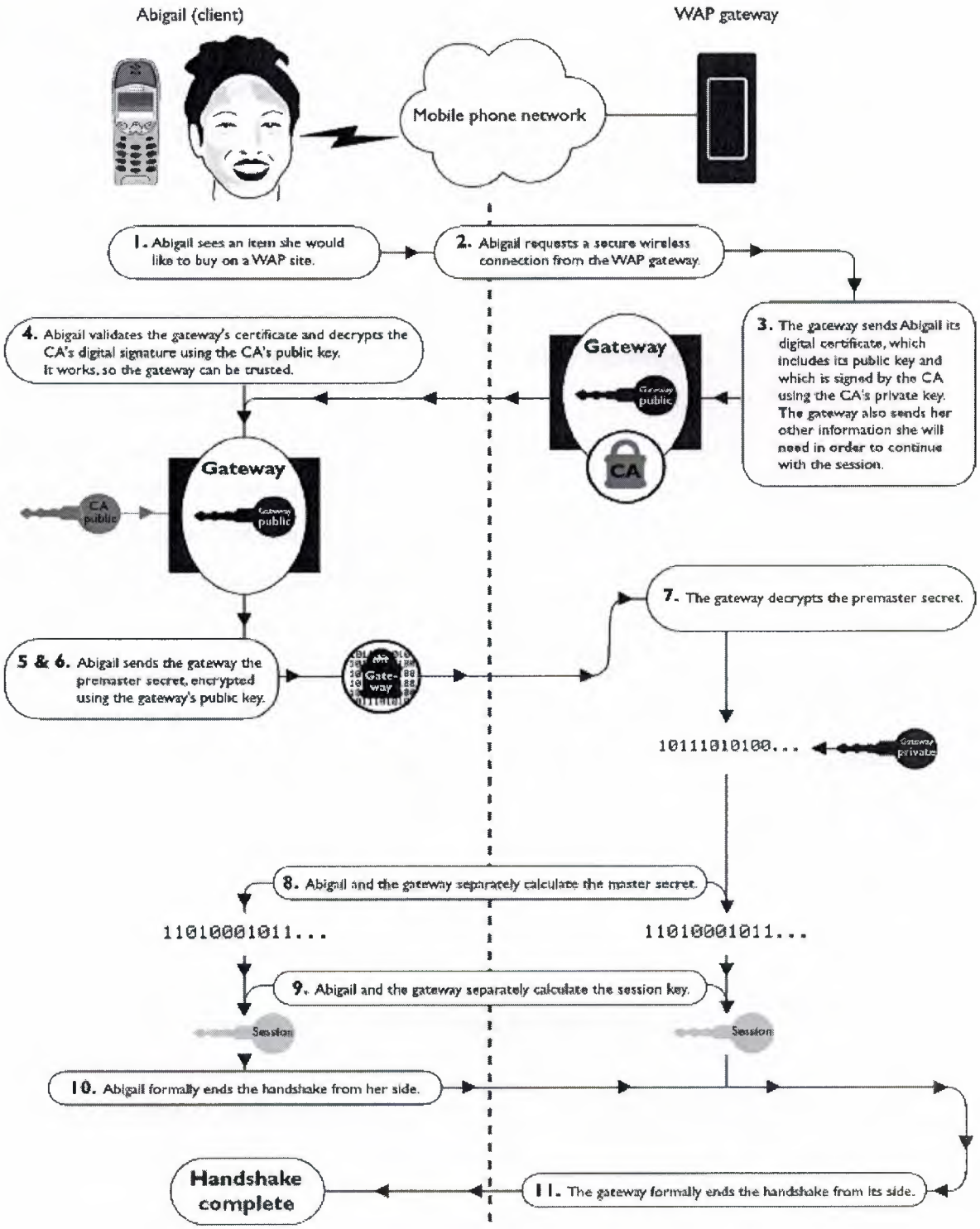

Figure 4.6 WTLS handshake

4.9.3 Digital Certificate Formats

WTLS specifies two possible formats for digital certificates:

- X.509. This is the standard format for digital certificates in SSL, and is optional in implementations of WTLS. However, it is not supported by the current generation of WAP client devices. The principal information contained in an X.509 certificate is:
- The subject's name
- The issuing CA's name
- The certificate's validity period
- The asymmetric and symmetric algorithms used for key exchange
- The subject's public key
- The digital signature of the issuing CA
- Alternative names for the subject (optional)
- Allowed key usage - for example, whether the subject's public key may be used for Encryption, server authentication, signing other certificates, and so on (optional)
- WTLS. WTLS certificates are similar to X.509 certificates but more compactly coded, So as to suit the high latencies and low bandwidth of wireless networks, and the limited processing resources of WAP client devices. WTLS certificates also omit some of X.509's non-essential fields, such as alternative subject names and key usage options.

A WTLS certificate includes the following information

- The subject's name
- The issuing CA's name
- The certificate's validity period
- The asymmetric and symmetric algorithms used for key exchange
- The subject's public key
- The digital signature of the issuing CA

4.9.4 Certificate Revocation In WTLS

On the terrestrial Internet, a CA can revoke a certificate it has issued before the end of the certificate's validity period, if the security of the owner's private key has been compromised or if there is new reason to doubt the owner's identity or integrity Certificate revocation on the terrestrial Internet is implemented by means of certificate revocation lists issued by CAs. When an Internet client receives a certificate from a secure server, it retrieves the signing CA's certificate revocation list from the Internet, checks that the certificate does not appear it, and if not, accepts the certificate. On the Mobile Internet, it is impracticable for a small client device to check a revocation list every time it downloads a gateway's certificate. The problem of revocation is therefore addressed by the use of short-lived certificates. The CA, instead of issuing the secure WAP gateway with a single certificate valid for a long period, sends it a fresh certificate at short intervals throughout that period - for example every 25 hours. Each certificate is only valid until the next one arrives. If the CA needs to revoke its endorsement of a gateway (for example, because the security of the gateway's private key has been compromised), it simply stops sending the gateway certificates. Clients of the gateway will begin receiving expired certificates, and therefore will know that its security can no longer be relied on.

4.10 WTLS In Alligata Secure

4.10.1 Supported WTLS Implementation Classes

Alligata Secure supports all three WTLS implementation classes.

4.10.2 Supported Digital Certificate Formats

Alligata Secure supports both X.509 and WTLS certificates. Note, however, that X.509 certificates aren't currently supported by WAP client devices.

4.10.3 Supported Encryption Algorithms

Alligata Secure supports asymmetric keys generated by the RSA algorithm and symmetric keys generated by the MC5 algorithm

4.11 End-To-End Mobile Internet Security

As we have seen, WTLS provides security between the client device and the WAP gateway. Most secure Mobile Internet transactions will also require security between the WAP gateway and the HTTP server. This can be implemented using one of two arrangements

- SSL can be used between the gateway and the HTTP server. This method presents a Very slight security risk, because data is momentarily held unencrypted inside the gateway (a phenomenon known as the 'WAP Gap'). It is therefore important that administrative access to the gateway is strictly limited, that the relationship between the gateways host and the content provider is strong and trusting, and that the decrypted data is never stored outside the gateway's memory. This set-up is not recommended for operations requiring guaranteed security, such as online banking.

- The gateway can be hosted by the content provider and placed behind the content Provider's firewall. This set-up obviates both the 'WAP Gap' and the need for SSL between the gateway and the HTTP server. The content provider can, if they want, act as an Internet service provider (ISP) to the whole of the Mobile Internet, once the secure transaction is over. Alternatively, the content provider can close the secure WAP connection after the secure transaction has taken place, in which case the client user must dial in to their usual gateway in order to view other WAP sites. Figure 4.7 outlines a secure Mobile Internet transaction of the second type, with the WAP gateway behind the content provider's firewall. Abigail is now the user of a WAP client device, communicating with Brian via the WAP gateway.

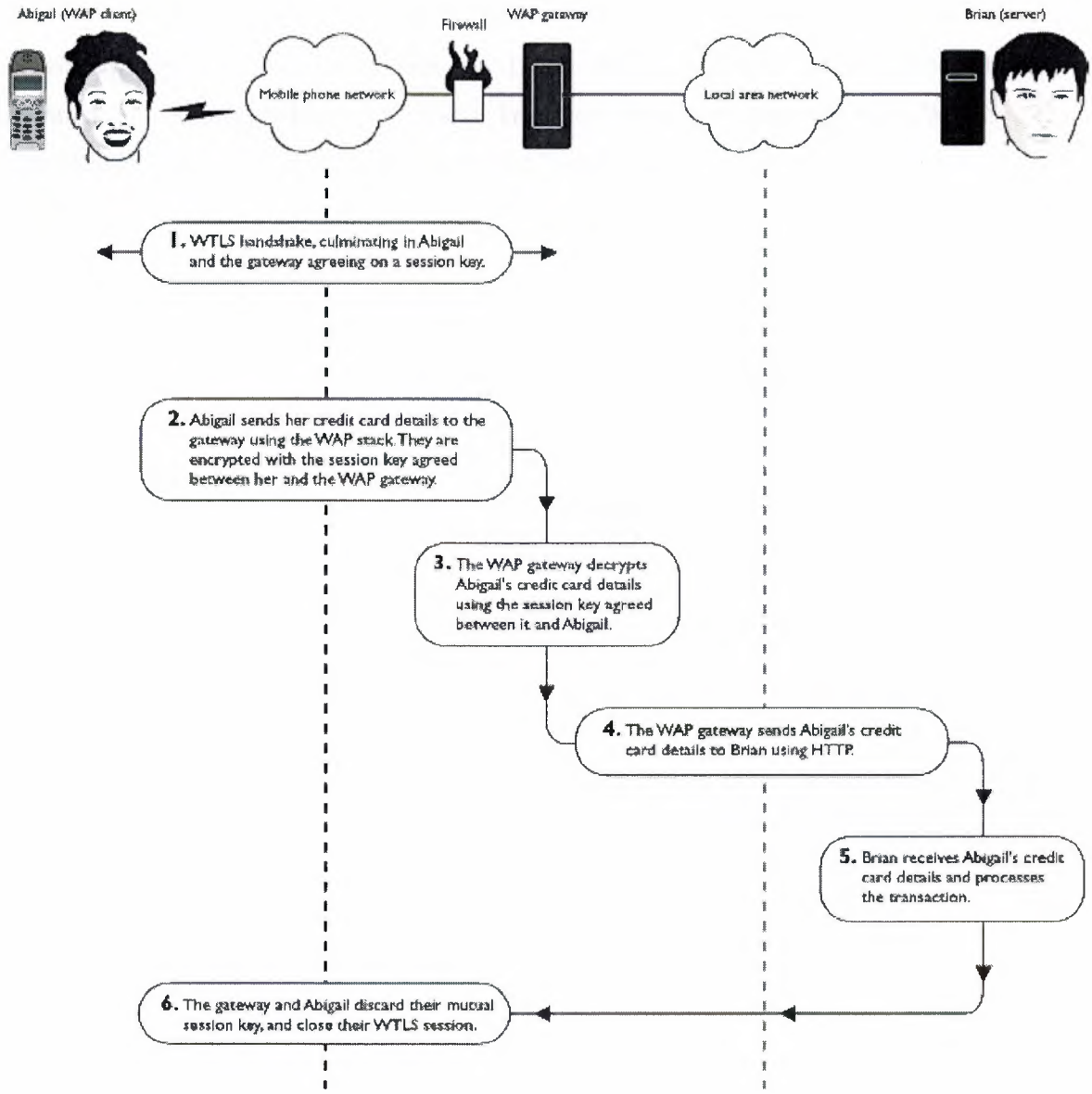

Figure 4.7 WTLS transaction, with the WAP gateway hosted by the content provider

4.12 Summary

In this chapter we discussed Internet Security Overview, Aspects of Internet Security, Insecurity of the Internet, Secure Sockets Layer (SSL), Privacy, Integrity Protection, Authentication, Non-repudiation, Wireless Transport Layer Security (WTLS),WTLS in Alligata Secure and End-to-End Mobile Internet Security,

Conclusion

Security, in the context of telecom networks, concerns all parties involved: the end-user, the service provider, the content provider, the applications provider, and the operator. The concerns can be expressed in terms of loss of service, loss of revenue and image, loss of confidentiality, mistrust, churn, and possible legal actions. Security is not a static procedure that can be applied once and for all. It is a living process that grows with the network, users, applications, technology and offenders. Security should be addressed with technical, administrative, procedural and technical counter measures, the primary components of a successful security strategy are:

- Policy: define security objectives, principles and compliance.
- Auditing: thoroughly verify if policies are enforced effectively.
- Detection: watch for violations and fraud on a regular basis.
- Protection: implement safeguards to minimize risks to critical assets.
- Testing: to ensure proactive security measures remain effective.

Only when structured approaches including these components are strictly followed,
A sufficient security level can be achieved and maintained.

REFERENCES

1. ISSPCS Practitioner Reference Communications and Network Security Functional http://www.isspcs.org/

2. ISSPCS Practitioner Reference Systems Security Functional Discipline http://www.isspcs.org/resources/.

3. "Security Architectures for mobile networks" http://www.ericsson.com/about/publications/review/2004_02/files/2004125.pdf

4. "Mobile Platform Security" http://www.ericsson.com/ericsson/corpinfo/publications/review/2006_02/files/mobile platform_security.pdf

5. "Security architecture for systems providing end-to-end communications" https://www.ietf.org/IESG

6. A Comparison of Security in Home RF versus IEEE802.11b. (2001). the World Wide Web http://www.homerf.org/data/tech/security_comparison.pdf

7. A Comparison of Security in Home RF versus IEEE802.11b. (2001). Retrieved November 1, 2001 from the World Wide Web http://www.homerf.org/data/tech/security_comparison.pdf

8. Adobe, B. (2001). IP sec-NAT Compatibility Requirements, Internet Engineering Task Force (IETF), IP Security Protocol (ipsec) Working Group, Internet Draft. Retrieved October 11, 2001 from the World Wide Web http://www.ietf.org/internetdrafts/Draft-ietf-ipsec-nat-reqts-00.txt

9. Blake-Wilson, S., Nystrom, M. (2000). Wireless Extensions to TLS, Internet Engineering Task Force (IETF), Transport Layer Security (tls) Working Group, Internet Draft. Retrieved June 6, 2001 from the World Wide Web http://www.ietf.org/internet-drafts/draft-ietf-tls-wireless-00.txt

10. Borisov, N., Goldberg, I., & Wagner, D. (2001).Intercepting Mobile Communications: The Insecurity of 802.11. Retrieved September 21, 2001 from the World Wide Web http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf

11. [CERT2001] Kevin J. Houle and George M. Weaver. Trends in Denial of Service Attack Technology. Computer Emergency Response Team (CERT) Coordination Center. http://www.cert.org/archive/pdf/DoS_trends.pdf

12. [CSE1999] Communications Security Establishment (Canada). Common Criteria Version 2.1: An Introduction. 1999-09
http://www.csecst.gc.ca/cse/criteria/english/docs/brochure.pdf
13. [Ranum1996] Marcus J. Ranum. Internet Attacks. 1996.
http://pubweb.nfr.net/~mjr/pubs/attck/index.htm
14. [Saltzer1975] Jerome H. Saltzer and Michael D. Schroeder. The Protection of Information in Computer Systems. Proceedings of the IEEE, vol. 63, no. 9 (1975-09), pp. 1278-1308.
http://web.mit.edu/Saltzer/www/publications/protection
15. [SANS2001] the System Administration, Networking, and Security (SANS) Institute. The Twenty Most Critical Internet Security Vulnerabilities: The Experts' Consensus.
http://www.sans.org/top20.htm