DESIDOC Bulletin of Information Technology, Vol. 24, No. 2, March 2004, pp. 9-16

Networking and Security Measures

Vaibhav Gupta, Sumit Goswami, Ashok Kumar & Mohinder Singh

Abstract

By writing this paper a small effort has been put to understand the growing network needs and its security. Various types of network threats and security services are discussed. This will help in designing a secure and robust network infrastructure by discussing management security policies and risk analysis.

1. INTRODUCTION

With the growing dependence on network to aid smooth communication and increased outputs, information Technology (IT) industry must become more concerned about the possible security threats that can breach network security resulting in costly damages. This paper discusses why a growing network must be secure.

To make network secure it is essential to understand what is a network and what are the components that forms the network. In brief, a network may be described as interconnections of autonomous nodes, which are physically separated. These interconnected nodes may be routers, switches, firewalls, servers, etc. Many networks connected together, i.e., hybrid kind of network is called Internet. Internet is a vast bank of information shared among individuals in any part of the world without any physical geographic limitation. A network layout is as shown in figure 1.

The first thing to realize is that internet-world is a part of reality. The people we correspond with on the network are real people with lives, careers, habits and feelings of their own. These feelings sometime go

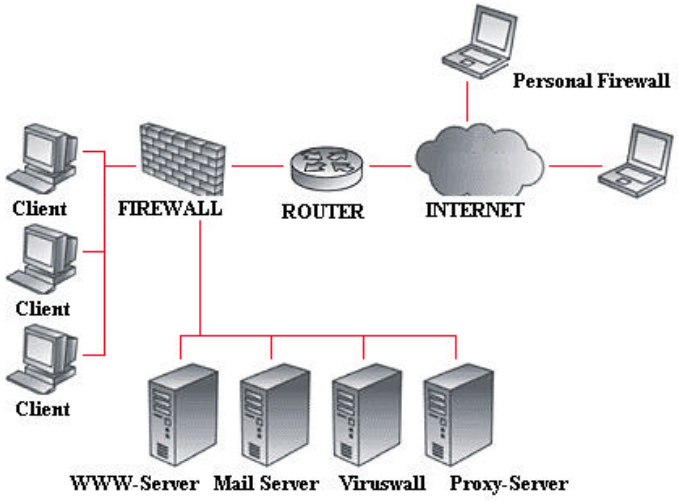

Figure1. Network Infrastructure

malicious and lead to network attack. The electronic part of life must be taken seriously. In particular, we should think about and consciously choose how we wish to use the network. Anyone engaged in many forms of communication on the net—one-to-one electronic correspondence, network discussion groups, web publishing, and so forth. These interactions might be employed as part of a wide variety of professional activities: sharing raw data, arguing about technical standards, collaborating on research projects, chasing down references, commenting on drafts of papers, editing journals, planning meetings and trips, and so on. All these activities must be carried out maintaining a certain level of security.

2. TYPES OF ATTACKS

There are a number of possible reasons for network attacks:

- A professional hacker with destructive mind could cause severe damage to a network.
- To come in limelight for recognition and appraise
- A company's competitor may cause such a attack
- In some cases, it is noticed that the internal employees are also responsible for network attacks.

The most susceptible attacks are fired on routers, switches and hosts. Host could be a web server, mail server, database server or even a firewall. Since, last decade there has been a great enhancement in network warfare. Hackers today are more proficient and aim at severe destruction. With this fast and vast growth of spreading computer network, the level of dependency has been increased tremendously.

The most common is the 'password attack'. These attacks are made through list word dictionary loops. Common words or default passwords are sent to the server by intruder to authenticate illegally. Sometimes, social engineering is also practiced where someone act as organisation employee on phone to obtain password.

A second type of attack is Denial of Service (DOS) in which unmanageable data is sent to the host thus making it incapable to handle and ultimately leads to network crash. Network attack may also happen due to loopholes in the operating system and network applications.

In recent years a number of Trojan attacks were reported due to loopholes left undetected.

3. LOSSES SUFFERED

Network attacks result in down time and costly damages. Breach in data confidentiality and integrity can result in loss from hundred to millions of rupees. E-shops may suffer loss in revenue as customers will move to other places. The informational websites may loose valuable advertisement time and form bad public relations. Replacing relevant information with non-sensical such as in Defence sites may cause insecurity and lack of confidence among citizens.

Table 1shows the recent survey done by First Coast Online (www.fcol.com/network_ security.htm) in 2001- 2002 indicating the number of network attacks and cost incurred on them to recover:

Table 1. Network Security by numbers 2001-2002

166 %	Increased in the number of attacks on Linux based web applications
7 out of 10	Portion of internet security attacks using port 80/HTTP
2796.5 Billion Rs.	Annual cost of software bugs to developers and users
21 %	Overall cost savings when security is addressed in the design phase of a product or network development cycle
30.2 %	Portion of 149 surveyed IT organisations that have identified rogue wireless APS on their networks

4. DESIGNING SECURITY INFRASTRUCTURE AND ARCHITECTURE

Designing of security infrastructure becomes essential. In designing a security infrastructure a cost/benefit analysis must be done, which may involve calculation of cost of recovery. To accomplish this task, security policies must be framed by highest level of management considering security requirements, implementation of guidelines regarding available technology and time-to-time updation of security policies if desired.

Once, security infrastructure is designed next comes is the security architecture which is developed from network design and its security team. In this the access and security requirements must be set and divided into layers of security so as to prevent an expert intruder and get trapped in these layers.

4.1 Security Services

Some security services must be implemented such as password authentication, authorization and accounting. In the days of localized, centrally managed systems, passwords were considered sufficient to validate and authenticate users. Over today's distributed and untrusted networks, passwords are sniffed, stolen, shoulder-surfed or too easy for the determined attacker to guess. To take care of it comes Strong User Authentication (SUA), a move to develop more secure authentication systems that are not susceptible to the many weaknesses of simple password systems. SUA augments systems uses combinations to form passwords (something that is not easy to guess) with a possession. The most notable SUA systems are token-based and biometric authentication systems. Biometric authentication systems (using unique biological traits) continue to develop as the industry attempts to identify a standard that will guarantee interoperability. Token-based security systems have been on the market for approximately a decade and have been proven in numerous environments. Options are available for practically any platform--desktop or server that can be imagined. These systems interface nicely with standardized protocols, including RADIUS (Remote Authentication Dial-In User Service), TACACS (Terminal Access Controller Access Control System) or TACACS+. In fact, many network hardware vendors now provide built-in support for a number of token-authentication services

A separate level of access for different class of users must be defined alongwith access right i.e., trust model. Virtual private networks confidentiality must be maintained and security monitoring by Intrusion Detection System (IDS). Deployment of security architecture involves defining of critical areas. Many intrusion detection systems base their operations on analysis of OS audit trails. This data forms a footprint of system usage over time. It is a convenient source of data and is readily available on most systems. From

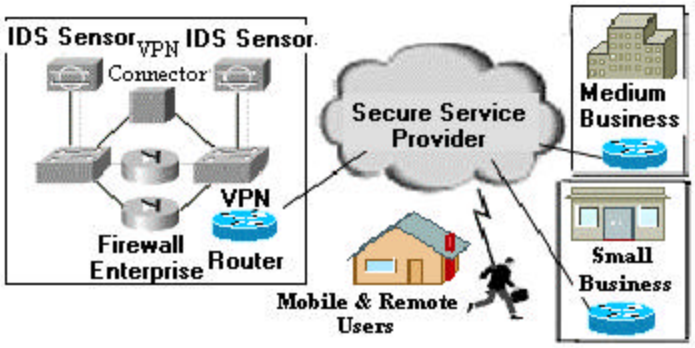

Figure 2. Intrusion Detection System

these observations, the IDS will compute metrics about the system's overall state, and decide whether an intrusion is currently occurring.

IDS may also perform its own system monitoring. It may keep aggregate statistics, which gives a system usage profile. These statistics can be derived from a variety of sources such as CPU usage, disk I/O, memory usage, activities by users, number of attempted logins, etc. These statistics must be continually updated to reflect the current system state. They are correlated with an internal model, which will allow the IDS to determine if a series of actions constitute a potential intrusion. This model may describe a set of intrusion scenarios or possibly encode the profile of a clean system

5. SECURITY TECHNOLOGIES

Determining level of implementation investment must incorporate latest security technologies. The procurement involves deciding allocation of available network security budget to adequately secure the network. The very first step involves the identification of network users, hosts, applications, services and resources and the access levels. Then comes the control access to these network applications and services through routers, switches and firewalls. Some complementary tools such as virus scanners and content filters can also be included for perimeter security.

5.1 Secure Connectivity

Secure connectivity must be established for protection of information transmission. The information transmitted must be in encrypted form. Digital signatures can be used to encrypt the information. Encryption technology converts network messages into formats that are specially designed to prevent third parties from accessing their contents. The process of encryption hides data or the contents of a message in such a way that the original information can be recovered through a corresponding decryption process. Encryption and decryption are common techniques in cryptography, the scientific discipline behind secure communications. Modern web browsers use the Secure Sockets Layer (SSL) protocol for secure transactions like e-commerce purchases and banking. SSL works by using a public key for encryption and a different private key for decryption. Virtual Private Network (VPN) (figure 3) must be established for private secure communication across public network

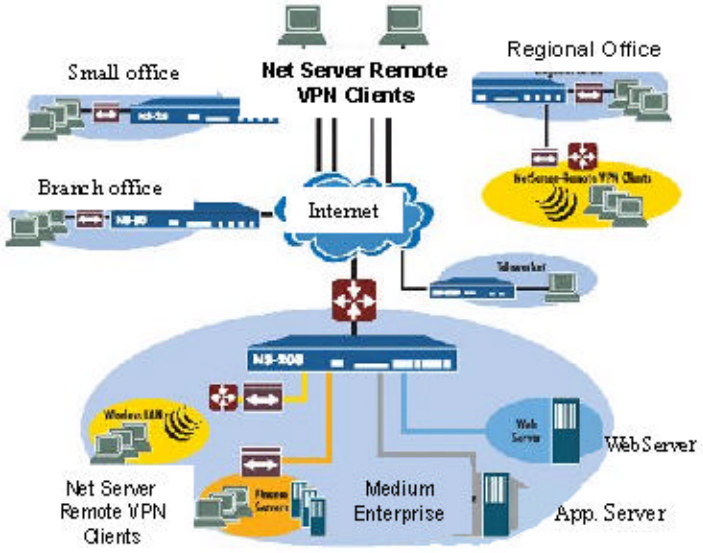

Figure 3. Virtual Private Network

such as internet, enabling corporate network extension to remote offices, mobile users and telecommuters.

5.2 Security Monitoring

Besides secure connectivity security monitoring is also essential. Continuous monitoring of network for safeguard against attacks test security infrastructure. The log files of the users accessing the host containing information about their IP addresses, duration and time stamp must be recorded. The weak areas must be identified through intrusion detection systems and the network security holes must be fixed before hackers find them. Figure 4 shows a network centre.

6. SECURITY POLICY MANAGEMENT

At last, the security policy management is done, where centralized security policy management tools and auditing security policy tools are applied. These policies must identify IP security and VPN security through IDS and implementation of firewall. As building a good security policy provides the foundations for the successful implementation of security related projects in the future, this is without a doubt the first measure that must be taken to reduce the risk of unacceptable use of any of the organisation's information resources.

The first step towards enhancing an organisation security is the introduction of a precise yet enforceable security policy, informing staff on the various aspects of their responsibilities, general use of organisational resources and explaining how sensitive information must be handled. The policy will also describe in detail the meaning of acceptable use, as well as listing prohibited activities.

The development and the proper implementation of a security policy is highly beneficial as it will not only turn all of the staff into participants in the organisation's effort to secure its communications but also help reduce the risk of a potential security breach through 'human-factor' mistakes. These are usually issues such as revealing information to unknown (or unauthorized sources), the insecure or improper use of the internet and many other dangerous activities.

Additionally the building process of a security policy will also help to define organisation's critical assets, the ways they must be protected and will also serve as a centralized document, as far as protecting information security assets is concerned.

The security policy is basically a plan, outlining what the organisation's critical

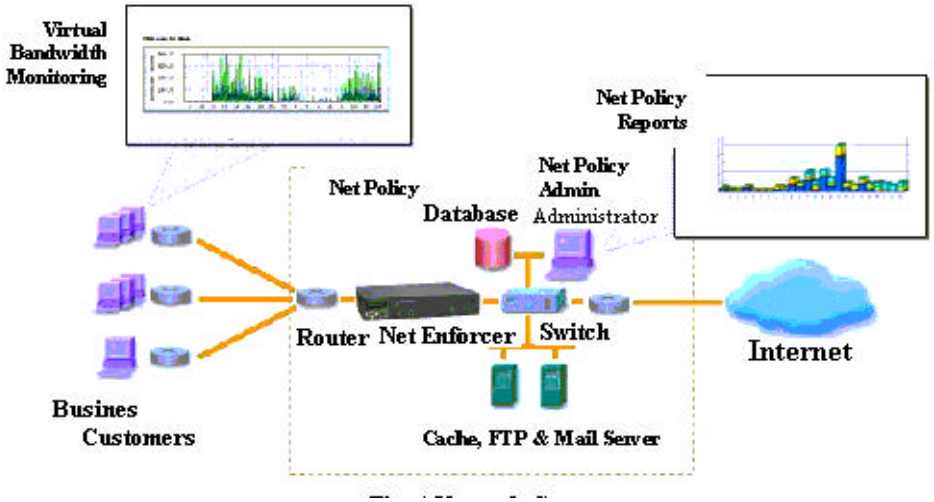

Figure 4. Network Centre

assets are, and how they must and can be protected. Its main purpose is to provide staff with a brief overview of the acceptable use of any of the information assets, as well as to explain what is deemed as allowable and what is not, thus engaging them in securing the organisation's critical systems.

The document acts as a 'must read' source of information for everyone using in any systems and resources defined as potential targets. A good and well-developed security policy should address some of these following elements:

- How sensitive information should be handled
- How to properly maintain your ID(s) and password(s), as well as any other accounting data
- How to respond to a potential security incident, intrusion attempt, etc.
- How to use workstations and internet connectivity in a secure manner
- How to properly use the corporate e-mail system.

Basically, the main reasons behind the creation of a security policy is to set a organisation's information security foundations, to explain to staff how they are responsible for the protection of the information resources, and highlight the importance of having secured communications while doing business online.

7. RISK ANALYSIS & MANAGEMENT

As in any other sensitive procedure, risk analysis and risk management play an essential role in the proper functionality of the process. Risk analysis is the process of identifying the critical information assets of the organisation and their use and functionality, an important (key) process that needs to be taken very seriously.

Essentially, it is the very process of defining exactly 'What is to protect', 'from Whom trying to protect', it and most importantly, 'How it will be protected'.

In order to be able to conduct a successful risk analysis, we need to get well acquainted with the ways a organisation operates; if applicable, the ways of working and certain business procedures, which information resources are more important than others (prioritizing), and identifying the devices/ procedures that could lead to a possible security problem.

Everything that is essential for the proper functionality of the business processes should be listed; like key applications and systems, application servers, web servers, database servers, various business plans, projects in development, etc.

A basic approach would be:

- Identify what is to protect
- Look at from whom to protect.
- Define what are the potential risks involved
- Consider monitoring the process continually in order to be up to date with the latest security weaknesses.

A possible list of categories to look at would be:

- **Hardware**: All servers, workstations, personal computers, laptops, removable media (CD's, floppies, tapes, etc.), communication lines, etc.
- **Software**: Identify the risks of a potential security problem due to outdated software, infrequent patches and updates to new versions, etc. The potential issues with staff installing various file sharing applications (Kazaa, Sharereactor, E-Donkey, etc.), IM (chat) software, entertainment or freeware software coming from unknown and untrustworthy sources should also be taken into account.
- **Personnel**: Those who have access to confidential information and sensitive data.

7.1 Physical/Desktop Security

For creating a strong network environment, the organisation should adhere to the following steps strickly:

- **System Access**

Best practices for password creation, passwords aging, minimum password length, characters to be included while choosing passwords, password maintenance, tips for safeguarding (any) accounting data; the dangers to each of these issues must be determined and thoroughly explained.

- **Virus Protection**

Best practices for malicious code protection, how often the system should be scanned, how often, if not automatically, should Live Update of the software database be done, tips for protection against (any) malicious code(viruses/trojans/worms) must be elucidated.

- **Software Installation**

Software Installation is freeware software forbidden, if allowed, under what conditions, how is software piracy tolerated, are entertainment/games allowed or completely prohibited as well the installation of any other program coming from unknown and untrustworthy sources must be dealt carefully.

- **Removable Media (CD's, floppy)**

'Acceptable Use' measures (perhaps by way of a Acceptable Use Policy (AUP) need to be established.

The dangers of potential malicious code entering the organisation network or any other critical system through floppies, CDs are other form of media need to be explained as well.

- **System Backups**

The advantage of having backups needs to be explained; who is responsible for data backup.

How often should the data be backed up, selection of storage device and the place where the backup to be kept must be decided.

- **Maintenance**

The risks of a potential physical security breach must be foreseen; complete identity of the person accessing the system is essential, FDD locks, identity cards and bio traits must be implemented.

- **Incident Handling**

Define what a suspicious event is, to whom it needs to be reported, and what further steps need to be taken must be decided in advanced.

7.2 Internet Threats

- **Web Browsing**

Define what constitutes restricted, forbidden and potentially malicious web sites, provide staff members with brief, and well summarized tips for safer browsing, additionally let them know that their internet usage is strictly monitored in order to protect organisation's internal systems.

- **E-mail Use**

Define the 'acceptable use' criteria of the E-mail system, what is allowed and what is not, the organisation policy on using the mail system for personal messages, etc.

Also briefly explain the potential threats posed by (abusing) the mail system and of the potential problems as far as spreading malicious code is concerned.

- **Instant Messaging (IM) Software (ICQ, AIM, MSN, etc.)**

Whether it is allowed or completely forbidden, provide them with short examples of how an attacker might use these programs to penetrate and steal/corrupt/modify organisation data.

- **Downloading/Attachments**

Is downloading allowed or not, useful tips for safer downloading, explanation of trusted and untrustworthy sources, best practices for mail attachments if allowed, discussion of potential threats and dangers, use of virus scanners, etc.

Staff need to understand why some activities are prohibited, what the impact of certain dangers can have on the organisation, actions they must follow if and when a potential security problem has been suspected or discovered.

By involving staff in a security awareness programme, the concerned staff will not just broaden their knowledge on the information

security field, but also learn how to act in a secure manner while using any of the organisation's information assets.

CONCLUSION

The aim of this paper is to explore the process of building and implementing a successful, secure and robust network infrastructure. We have discussed various techniques to overcome possible security threats. The security process require constant monitoring of the network alongwith the measurement of staff knowledge and awareness levels to ensure that there is a continuous improvement in their level of security knowledge and awareness.

REFERENCES

1. LaPadula, L.J. Proposed network security policy for integrated tactical warning and attack assessment system. NTIS, Virginia, 1993.
2. Hampel, Viktor E. Information protection and network security. SPIE, Washington, 1996.
3. Shaffer, Steven L.; & Simon, Alan R. Network security. AP Professional, Boston, 1994.
4. Stallings, William. Cryptography and network security: Principles and practice. Prentice Hall, New Jersey, 1999.
5. Kaufman, Charlie; Perlman, Radia; Speciner, Mike. Network security: Private communication in a public world. Prentice Hall, New Jersey, 1995.
6. Kaeo, Merike. Designing network security. Techmedia, New Delhi, 1999.
7. Canavan, John E. Fundamentals of network security. Artech House, London, 2001.

Contributors: **Dr. Mohinder Singh**, Director, Defence Scientific Information and Documentation Centre (DESIDOC), Metcalfe House, Delhi - 110 054.
Sh. Ashok Kumar, Scientist 'E', DESIDOC, Delhi - 110 054.
Sh. Sumit Goswami, Scientist 'C', DESIDOC, Delhi - 110 054.
Sh. Vaibhav Gupta, STA 'A', DESIDOC, Delhi - 110 054.