Provision of Security in Operating Systmes

Rashmi Bhatia
Dept. of Computer Applications
Dev Samaj College for Women
Chandigarh, India

Abstract—Security is a paramount requirement of the age. Information stored in the form of bits than as atoms of ink and paper traveling near the speed of light, may be duplicated without limit and with insignificant cost. In today's environment, establishing a framework for the authentication of computer-based information requires a familiarity with concepts and professional skills from both the legal and computer security fields

This paper represents various threats to the system and measure to protect the system from these threats and attacks. With explaining the Protection and Security measures provided in an operating system.

Keywords—authentication; authorization; brute force; trojan horse; virus; encryption

I. INTRODUCTION

In an Operating System, there are various users, who share either the programs or the data lying on the system. That is why a lot of risk is involved. There is a need of protection and security measures in an operating system.

Protection can be defined as “guarding a user’s data and programs against interference by internal entities of a system, viz. other authorized users of the system”. (Dhamdhere, D.M., 2001, p.588).

Security can be defined ad “guarding a user’s data and programs against interference by entities external to a system, e.g. unauthorized persons”. (Dhamdhere, D.M., 2001, p.588).

So an operating system has to apply safeguards against the internal as well as external interference to a system. That is why protection and security go together.

II. DANGERS TO A SYSTEM

A system is prone to various dangers affecting the overall working of the system or misusing the information or making the information inconsistent. These can be described as follows: -.

A. Wrong User

Different users on network can login from any terminal on network can get access to the system. To handle each user, user’s identification for the system is required. This is made possible through user possession (a key or card), user knowledge (a user identity and password) and user attribute (fingerprint, retina pattern, or signature) etc. (Silberschatz et al., 2002)

But this will not solve the problem; rather it may lead to the breach of security, as

- Password may be either guessed by some other person.
- It can be illegally transferred from a misuse, as a result of the password compromise against bribe.
- Shoulder Surfing is possible, where the password of a user can be known by watching the keyboard.
- Sniffing or Eavesdropping is also possible through which anyone who has access over the network on which the system resides, can add a network monitor to listen the traffic of the network, capture the data packets, interpret, store them, and later on analysis are made on them. The important data like username, passwords, confidential reports, emails, documents can also be viewed.
- Password crackers are the programs, which apply “brute force; trying enumeration, or all possible combinations of letters, numbers, and punctuation (special characters), until the password is found” (Silberschatz et al., 2002). If the length of the password is short or if contains only lower caser or upper case letters or contains digits only, then it becomes more easier.
- Sometimes user may have a password difficult to guess or crack by the other person and difficult to remember can be stored somewhere else on the system can also be known by the other person, if he gets access to the system. Which may lead to
- Unauthorized read of data also known as the theft of information
- Unauthorized modifying the data
- Unauthorized destruction or deletion of data
- Preventing legitimate use of the system

B. Unauthorized Access of Resources

A file created by one user, very important for that user can be accessed, altered, deleted, or renamed by the other user who is not the owner of the file. Thus the owner of the file is in trouble. This is known as unauthorized access of resources. Thus there is a need of a mechanism, which provides different access rights on different resources to different users, which are also known as protection mechanisms against the system.

C. Program Threats

A code written by one user, may be misused by another user, can be described as program threats described as follows:

1) *Trojan Horse:* It can be defined as a code segment that misuses its environment. Trojan horse program is a useful program, containing hidden code, which after being invoked performs various unwanted functions. The author of the Trojan horse program, first of all, creates the source code of a useful program, which may attract the users and then add code, which makes the program to perform some harmful functions in addition to its useful functions. They appear to be harmless programs, which may enter into a computer system through any channel, but at the time of their execution, they install some other program on the computer that can be very harmful to the system (Walker, T.J., 1999).

Examples of the Trojans are: IRC.Sx2, Trifor, Sexy.exe (which formats hard disk)

2) *Trap Door:* It can be defined as an intentional hole in the software. The programmers sometimes leave a hole in the software intentionally, which is used by them only. An example of trap door is the hole left in the banking software by the programmers to have occasionally half-cent credited to their accounts. Sometimes rather than adding a trap door to the source code of the program, it can be added in the source code of the compiler. Thus on compiling the program, the object code plus trap door are generated together. If one keeps on detecting the source code of the program, no trap door would be found because trap door is in the compiler's source code. It is difficult to detect a trap door because analyzing all the source code for all the components of a system is quite difficult. (Silberschatz et al., 2002)

3) *Stack Overflow or Buffer Overflow:* In this case, the attacker overflows the input field or the buffer by sending more data than the program was expecting, which compels the program to write into the stack. "A malicious user may inject executable code in memory buffers belonging to the stack or the data segment of a process P. In addition, if the attacker manages to change the return address of a function, the fragment of code he injected is executed by P".(Bernaschi et al., 2002)

These are very hard to detect or prevent and can also bypass the security provide by the firewall.

D. System Threats

The operating system provides the processes with various means to spawn other processes, which may lead to the problem of system threats. This misuse is achieved by the following methods: -

1) *Worms*: A worm can be defined as "a standalone program that spawns other processes (copies of itself) to reduce system performance". (Reali, P. and Corti, M.). It causes the program to execute by itself without the intervention of the user.

Examples: - Morris Worm (1988), Mapson, Sobig.D, Trile.C, Lovgate.F, PSWBugbear.B

2) Viruses: "Viruses are similar to worms but embedded in other programs. They usually infect other programs and the boot sector" (Reali, P. and Corti, M.). These programs copy their hidden code to other programs, so as to infect them.

Features of a Virus: - According to Walker, T. J., 1999, a virus has three characteristics as follows:

- Replication Mechanism is the very first feature of the virus. As

➢ It searches for a program, which could be infected.
➢ After finding a program, a flag is checked to know whether the program has been infected previously.
➢ If it is an uninfected program, then the hidden code is inserted into the program
➢ Execution sequence is modified, so as to make the hidden code to be executed first.
➢ Adds a flag after infecting the program.

- Activation Mechanism checks for a certain action, the occurring of which results in the execution of the hidden code.

- Objective of the virus is to do some unwanted destructive event.

The most common types of viruses and their examples are: -

Table I. Types of Viruses

Virus type	Example
Overwrite Virus	Way, Try.Reboot, Trivial.88.D
Boot Virus	Polyboot.B, Anti.EXE
Macro Virus	Relax, Melissa.A, Bablas, 097M/Y2K
Polymorphic Virus	Tuary, SatanBug, Marburg, Elkern
Multipartite Virus	Ywing
Companion Virus	Stator, Terrax.1069, Asimov.1539
Email Virus	I Love You
Resident Virus	Randex, CMT, Meve, MrKlunky

3) *Logic Bombs:* They are not considered viruses because they do not replicate. They are not even programs in their own right but rather camouflaged segments of other programs

E. Security Problems of a System on Network

1) Denial-of-Service: This type of attack causes your computer to crash or to become so overloaded that you are unable to use it. This network based attack is implemented by

- Consuming the available bandwidth of the network, so as to overload the network.

- Initializing a large number of programs simultaneously
- Introducing resource starvation by consuming all of the system resources such as CPU, hard disk space, memory, printer etc.
- Manipulating the table entries in the router or domain name servers, so as to deny the legitimate users access.

2) Worms are also more potent on the network as they may reproduce themselves among systems and affecting the entire network badly

3) Transmission of virus is fast over a network.

4) Sniffing or Eavesdropping may be introduced.

5) Risk of breach of confidentiality, authenticity and integrity also survive over the network, at the time of the text communication of the network.

These problems can be severe until some mechanisms to control them are initiated by the operating system.

III. SECURITY MECHANISMS AGAINST THESE DANGERS

Absolute protection of the system from malicious abuse is not possible but yes, security measures can be taken at four levels: physical, network, human and operating system level. Here we are concerned with the operating system level of security where the system protects itself from accidental or purposeful breach of security. At the earlier times, the hardware of the system was not compatible to provide protection to allow the implementation of security feature. That is why the MS-DOS and Macintosh operating system provide very less security. But still the designers of these operating systems are trying hard to add new security features to these operating systems because now hardware for better security is available. But no doubt, it is easier to design an operating system with security feature than to add features in existing software. That is why Windows NT was designed to provide security features from the very beginning.

A. Authentication

By authentication, we mean that the user who is working on a computer system is authentic or legal one and is not a fraud. The methods adopted to authenticate a user are as follows: -

1) Password: Every user of the system is provided with a user id and password. If the password given by the user matches with the password stored for the respective user id, then the user is treated as a valid user. It provides an external level security to the system.

- Passwords can also be associated with resources. If the user is willing to user that resource, he should have the password to use that resource. Thus resources may be saved from unauthorized access. In the same way various access rights like read or write or delete can be associated with various passwords.
- This method is used in large number. But sometime it may lead to some problems like sniffing of password, shoulder surfing, guessing, accidental exposure, illegal transfer or cracking of the password is also possible, which is harmful for the system. Thus in order to enhance the security:

➢ System Generated Passwords are used, which as the name indicate are generated by the system, is a combination of letters, digits, punctuations etc, difficult to remember but yes are hard to guess or crack.

➢ Age Passwords are also used, in which the age of a password is decided by the system. Thus on the expiry of that time period user is forced to change the password.

➢ Reuse of the earlier password should also avoided by the operating system by maintaining the history of every new password. So that every time user gives a fresh password.

➢ After every session with the system, the password is changed either by system or by user. So that even if password is used by wrong person during one session could not be reused by him and the breach of security can also be traced.

2) Encrypted Password: The computer system keeps the password for every user with it only but it can be accessed by some other user. Thus in an operating system, the encrypted password should be stored. We have an example of Unix operating system, which uses an encryption algorithm, by which every password is encrypted. But the designer of such algorithm states that the decryption of the password is impossible. Thus every password is encrypted and then stored in a file.

Now to provide extra security the access to the file, in which passwords are stored, should also be restricted because a user having the copy of encrypted password, can crack the password by first applying the same encryption algorithm on all the words in the dictionary and then compare it with the encrypted password. If the password is from the dictionary, it can be cracked. Thus for extra security

- Password should not be very simple or dictionary word or very small but yes, easy to remember.
- For example: - “My Marriage Anniversary is on 7th August”. This phrase can be used to generate a password, taking every second character of the phrase. i.e. YANSNTU
- The file used to store encrypted passwords should only be accessed by the superuser.

3) One-Time Passwords: In this case

- the user is supplied with an algorithm, such as an function, which user always keep with him, known as secret, never exposed to the system or is never transmitted over a medium.
- At the time of login, the system gives a seed i.e. a random integer to the user. User applies this integer to the function and gets the result

- This result is supplied to the system as password
- On the other side, the system also applied that integer to the function supplied to the user and gets the result.
- Then this result is compared with the password giver by user
- If two matches, then the access to the system is granted.
- The secret is never changed and every time a new seed is supplied, so as to have a new password every time
- It provides a better security, as a password user once can't be reused later on.
- (Silberschatz et al., 2002)

4) Biometric Authentication: Kay, R. (2005) states that Biometric authentication is the verification of a user's identity by means of a physical trait or behavioral characteristic that can't easily be changed such as fingerprint. These solutions are regarded as the most foolproof or hardest to be forged/ spoofed. Biometric systems earlier were slow, intrusive and expensive but provide maximum security, whereas now, these are much faster and cheaper even.

Types of Biometrics: - Kay, R. (2005) describes few of the widely accepted biometrics as follows: -

- Signature Dynamics: They take in consideration the difference in pressure and the writing speed at various points while doing signature.
- Typing Patterns: At the time of typing the password. The intervals between characters, the overall speeds and patterns are taken into consideration for authentication.
- Eye Scans: In this case, two parts of the eye of the user i.e. the retina and the iris can be scanned, using different technologies.
- Fingerprint Recognition: As the fingerprints are unique, so fingerprints are used for authentication.
- Hand or Palm Geometry: The devices in this case measure the finger length, finger width, the line patterns, temperatures map and the angles of individual fingers.
- Voice Recognition: Here, rather than putting emphasis on speech to know what is being said, the voice pattern is compared against the stored voice pattern.
- Facial Recognition: Various facial features including upper outlines of eye sockets, areas around cheekbones, the sides of the mouth and the location of the nose and eyes are taken into consideration for authentication purposes.

5) Two-Factor Authentication: Any authentication mechanism, whether it is

- user password or Personal Identification Number (PIN),
- a security token or smart card,
- or a physical characteristic such as fingerprint or any other form of biometric.

have drawbacks. So security experts recommend using combination of two separate mechanisms, known as two-factor authentication.

For example: - use of a one-time password generator and Personal Identification Number (PIN) together. But, this authentication method requires expensive hardware and infrastructure changes.

B. Authorization

It provides the internal level of security by assigning of read, write, execute, delete access rights on resources to users, to guard resources created and supported by an application subsystem against misuse.

1) Domain of Protection: "A domain defines a set of objects and the types of operation that may be invoked on each object." (Silberschatz *et al.*, 2002, p.631). A process executing in a domain can use the resources in the way specified therein, and cannot perform any other operation on that object.

- Joint domains can exist, where access right(s) can be shared by more than on e-domain.
- Association between processes and domains can be

Static, where

- Set to resources available to a process is fixed throughout its lifetime.
- based on need-to-know principal.
- a domain can be modified in a way to have minimum required access rights.

Dynamic, where

- a process can switch from one domain to another.
- each process, user or procedure can be a domain.

2) Access Matrix: The domain of protection expressed in a matrix form is called access matrix, having domain as rows, objects as columns, and each entry consist of a set of access rights.

- Domain Switching is done by adding domains as objects of access matrix
- Access matrix can itself become an object
- Each entry of access matrix need to be protected.

3) Implementation of Access Matrix: The access matrix can be implemented in any of the following forms: -

- A Global Table consisting a set of ordered triples<domain, object, right-set>

- Access List for Objects, where every column of access matrix is treated as an access list for one object, thus each object consist of ordered pairs <domain, right-set>, discarding the empty entries.

- Capability Lists for Domains, where each row is associated with its domain. The security of all capabilities (physical name or address of object) ensures the security of the object form unauthorized access.

C. Security Against Intruder

Silberschatz et al., (2002) state the following are some Intrusion-Detection Systems (IDSs)

1) Signature-Based Detection/ Anomaly Detection:

- In Signature-Based Detection
  - ➢ Dangerous or unexpected behaviors are characterized and if any of these occurs, are detected.
  - ➢ Won't detect attacks not specified in the list.

- In Anomaly Detection, normal behavior is characterized and detection takes place if something other than these behaviors occurs.

2) Auditing and Logging: "a common method of intrusion detection is audit-trail processing, in which security relevant events are logged to an audit trail and then matched against attack signatures (in signature-based detection) or analyzed for anomalous behavior (in anomaly detection)". (Silbervhatz *et al.*, 2002. p.676).

e.g. windows NT ad Unix both provide auditing facility to detect intrusion.

3) Tripwire: "Tripwire is a tool to monitor file systems for added, deleted, or changed files, and to alert system administrators to these modifications" (Silbervhatz *et al.*, 2002. p.677).

It can't differentiate between authorized and unauthorized changes.

4) System-Call Monitoring: This mechanism characterizes normal system call behavior in an abbreviated form, traces the actual system-calls made, compare them against those characterized, to detect the anomalous behavior. (Silbervhatz *et al.*, 2002).

D. Cryptography

Cryptography is the branch of applied mathematics that concerns itself with transforming messages into seemingly unintelligible forms and back again. It constrains the potential sender and receiver of a message, transmitted over a network. It is based on secret called keys.

1) Data Encryption: "Cryptography is a technique of encoding (i.e. encrypting) and decoding (i.e. decrypting) messages, so that they are not understood by anybody except the sender and the intended recipient". (Godbole, P.K., 2002 p.103).

The sender converts the plain text i.e. the original message into the cipher text i.e. the encrypted message. Then receiver on the other side, after receiving the data decrypts the cipher text and gets plain text as a result.

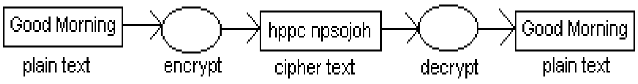

Figure 1: - Encryption and Decryption Process (Godbole, P.K., 2002)

The encoding and decoding is possible through and algorithm that should be agreed on by the communicating partied. This algorithm takes text as the input and then produces the encrypted text as an output and the message is transferred. The algorithm contains the intelligence for transformation of messages and that intelligence is called the key. Now, anybody having that intelligence i.e. the key can encrypt and decrypt the message.

Types of Encryption: - Godbole, P.K. (2002) suggests that on the basis of the key, encryption classified into two categories.

- Secret Key Encryption/ Private Key Symmetric Encryption: - In this case, one key is used for encryption and decryption both, and this key should not be known to anybody except sender and receiver.

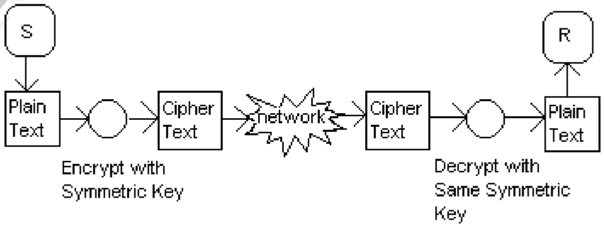

Figure 2: - Secret Key Encryption (Godbole, P.K., 2002)

Problems with this method are

  - ➢ Either the key is personally transferred, or through courier, post or through network, which involves risk of impression.
  - ➢ One key per communication party is required because same key can't be used for more than one party.

- Public Key Encryption/ Asymmetric Cryptography: - Two different keys are user, one for encryption known as public key and the other for decryption known as private key.

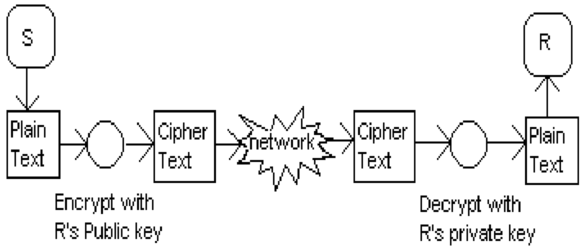

Figure 3: - Public Key Encryption (Godbole, P.K., 2002)

- ➢ The data encrypted by the public key can't be decrypted by one key other than the private key, not even by the same public key.
- ➢ Public key is known to anyone, willing to communicate. But private key is kept secret.
- ➢ The sender of message encrypt message with public key, transmit it to receiver and then the receiver decrypt the message with the private key.

Thus this method provides a better security than the previous one.

2) Digital Signature: A Digital code that can be attached to an electronically transmitted message that uniquely identifies the sender, to guarantee that the individual sending the message really is who he or she claims to be, is known as digital signature. Digital signatures use "public key cryptography".

- Digital signature Creation: -
  - ➢ S the sender encrypts the plain text into cipher text, using R's, the receiver's public key

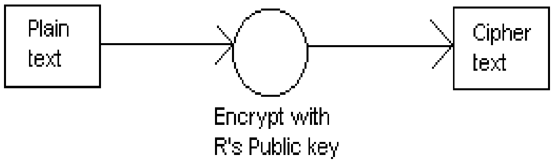

Figure 4: - Encryption Process (Godbole, P.K., 2002)

- ➢ S applies Hashing Algorithm on plain text, the result of which is the message digest. Then S encrypts the message digest with his own private key, for his authentication purpose.

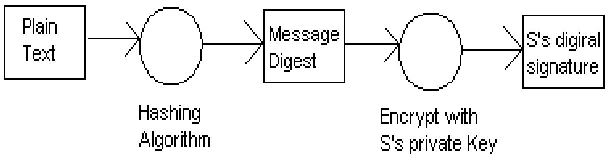

Figure 5: - Generating Digital Signature (Godbole, P.K., 2002)

- ➢ Digital Signature is appended to cipher text and message is transmitted to R.

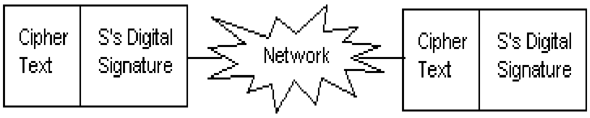

Figure 6: - Appending Digital signature to Message (Godbole, P.K., 2002)

- Digital Signature Verification: -
  - ➢ R decrypts cipher text, using R's private key and obtains plain text

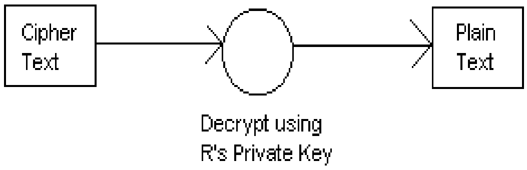

Figure 7: - Decryption process (Godbole, P.K., 2002)

- ➢ R obtains a message digest by decrypting S's digital signature.

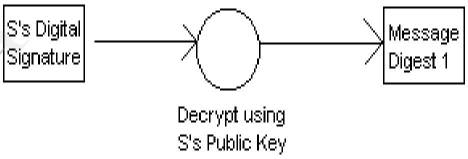

Figure 8: - Generating Message Digest From Digital Signature (Godbole, P.K., 2002)

- ➢ R creates message digest from plain text by applying the same hashing algorithm.

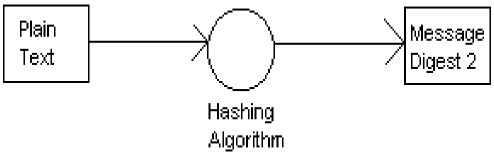

Figure 9: - Generating Message Digest From Message (Godbole, P.K., 2002)

- ➢ If both the message digest are same, then S is authenticated as a sender.

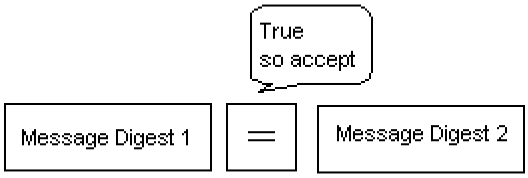

Figure 10: - Digital Signature Validatior (Godbole, P.K., 2002)

E. Providing Security To Systems On Network

The systems on network are more susceptible to security attacks, thus requiring more attention, explained as follows:

- A Top Secret system should be allowed to be accessed only form within a Top-Secure building or room. To make communication of that top-secret system with the external system, the connectors used should be securely locked in the safe.
- Scanners should be used periodically for scanning the security holes in system, when lesser workload is on the system, so as to check
  - ➢ The worms, viruses or other digital pests in the system
  - ➢ Unexpected overload on system
  - ➢ Unauthorized privileged programs
  - ➢ Any change in system programs
  - ➢ Short, simple, and easy-to-guess password
  - ➢ Damaged directory protections on user and system directories
  - ➢ Hidden or unknown network daemons.

These errors found can either be fixed automatically or reported to the system administration or both (Silbervhatz *et al.*, 2002).

- Sniffing can be avoided by using encrypted communication providing physical security over data communication closets or hubs on use of shard Ethernet etc.
- Stack or Buffer Overflow can be avoided if CPU disallows the execution of code in the stack portion of memory.
- Firewall: A firewall is a computer or router that sits between the internal secured environment and the external unsecured environment. Tanenbaum, A.S., (2002) states that firewall has two components: -

➢ Packet Filter: It is a standard router, that inspects every incoming or outgoing packet, according to some criterion, not fulfilling of which results in dropping of packet.

➢ Application Gateway: "Rather than just looking at raw packets, the gateway operates at the application level. A mail gateway, for example, can be set up to examine each message going in or coming out". (Tanenbaum, A.S., 2002, p.411).

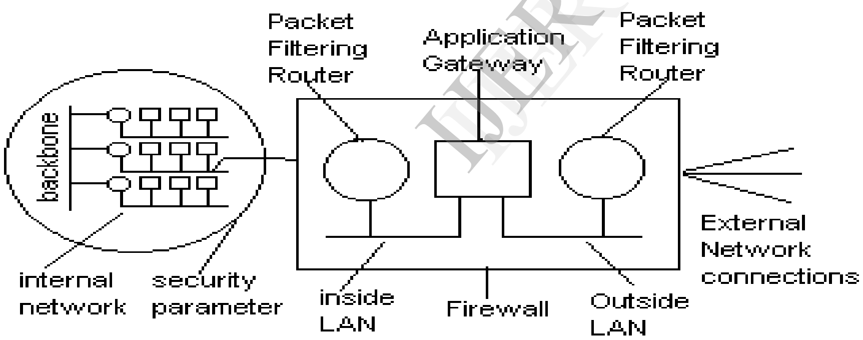

Figure 11: - Firewall with Application Gateway and two Packet Filters (Tanenbaum, A.S., 2002)

REFERENCES

[1] A. Silberschatz, P.B. Galvin and G. Gagne, Operating Systems Concepts, 6th ed., Singapore: John Wiley & Sons (Asia) Pte. Ltd., 2002.

[2] D.M. Dhamdhere, Systems Programming and Operating Systems, 2nd revised ed., New Delhi: Tata Mcgraw-Hill Publishing Company Limited, 2001.

[3] A.S. Tanenbaum, Computer Networks, 3rd ed., New Delhi: Prentice-Hall of India Private Limited, 2002.

[4] K. Thakkar, K. Dattani, R. Mirchandani and A. Malani, Working With Unix, New Delhi: BPB Publications, 1993.

[5] Dulaney, Windows NT Server 4.0, New Delhi: BPB Publications, 1999.

[6] P.K. Godbole, Data Communications and Network, New Delhi: Tata Mcgraw-Hill Publishing Company Limited, 2002.

[7] R. Kay, Quick Study: Biometric Authentication [online], Computer World inc., <http://www.computerworld.com/s/article/100772/Biometric_Authentication?taxonomyId=017>.

[8] T.J. Walker, Computer Viruses and Related Threats [online]. <http://virii.es/C/Computer%20Viruses%20and%20Related%20Threats.pdf>

[9] Information Security Guidelines for NSW Government Part 2, Examples of Threats and Vulnerabilities [online]

<http://www.albany.edu/acc/courses/ia/inf766/nswinfosecriskmanagementpt21997.pdf>

[10] P. Reali and M. Corti, Addendum: Security [online], <http://www.cs.inf.ethz.ch/37-201/slides/SSW04_10_Security_6x.pdf>

[11] N. Bernaschi, E. Garbrielli and L. Mancini, REMUS A Security-Enhanced Operating System [online],

<http://www.researchgate.net/publication/220593675_Remus_a_security-enhanced_operating_system>