A

Seminar report

On

Cryptography and Network Security

Submitted in partial fulfillment of the requirement for the award of degree
of Bachelor of Technology in Computer Science

SUBMITTED TO:
www.studymafia.org

SUBMITTED BY:
www.studymafia.org

Acknowledgement

I would like to thank respected Mr…….. and Mr. ……..for giving me such a wonderful opportunity to expand my knowledge for my own branch and giving me guidelines to present a seminar report. It helped me a lot to realize of what we study for.

Secondly, I would like to thank my parents who patiently helped me as i went through my work and helped to modify and eliminate some of the irrelevant or un-necessary stuffs.

Thirdly, I would like to thank my friends who helped me to make my work more organized and well-stacked till the end.

Next, I would thank Microsoft for developing such a wonderful tool like MS Word. It helped my work a lot to remain error-free.

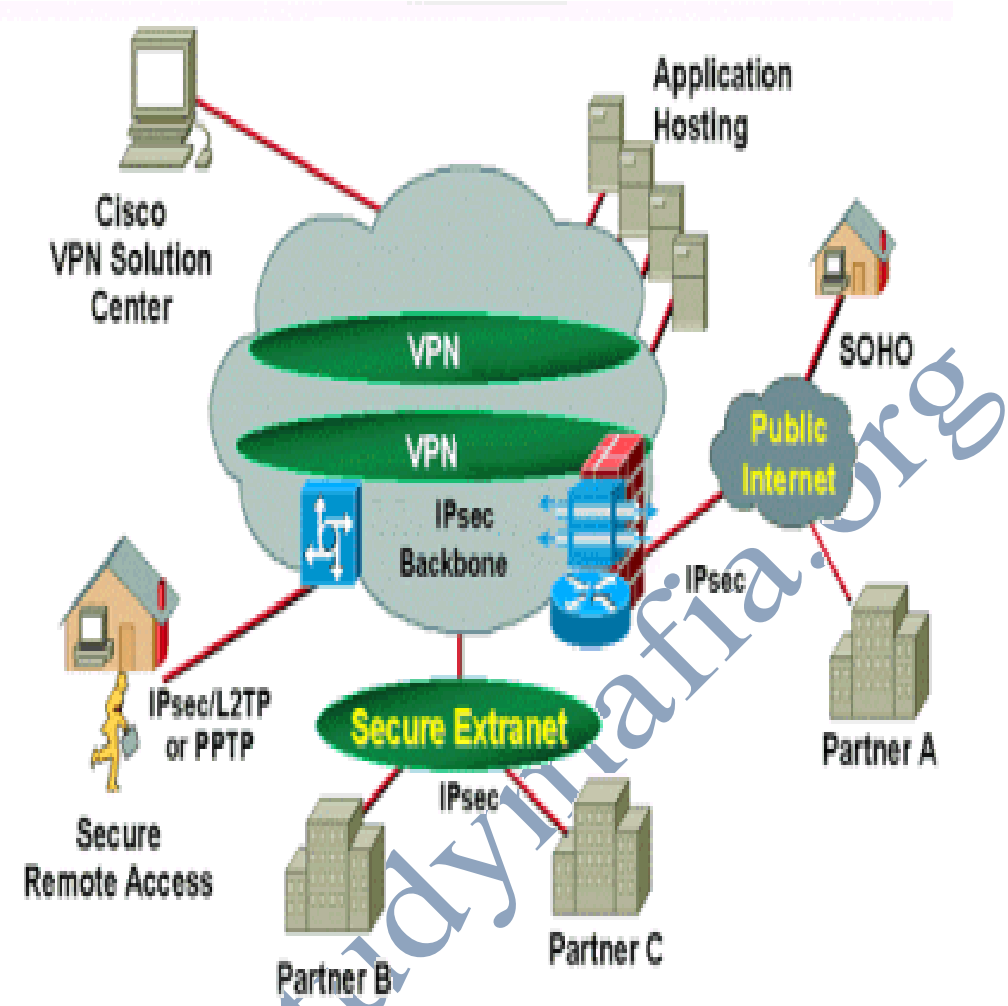
Last but clearly not the least, I would thank The Almighty for giving me strength to complete my report on time.

Preface

I have made this report file on the topic **Cryptography and Network Security** ; I have tried my best to elucidate all the relevant detail to the topic to be included in the report. While in the beginning I have tried to give a general view about this topic.

My efforts and wholehearted co-corporation of each and everyone has ended on a successful note. I express my sincere gratitude to ……..who assisting me throughout the preparation of this topic. I thank him for providing me the reinforcement, confidence and most importantly the track for the topic whenever I needed it.

Contents:



CRYPTOGRAPHY AND NETWORKSECURITY

ABSTRACT

"SECURITY" in this contemporary scenarios has become a more sensible issue either it may be in the "REAL WORLD" or in the "CYBER WORLD". In the real world as opposed to the cyber world an attack is often preceded by information gathering. Movie gangsters "case the joint"; soldiers "scout the area". This is also true in the cyber world. Here the "bad guys" are referred to as intruders, eavesdroppers, hackers, hijackers, etc. The intruders would first have a panoramic view of the victims network and then start digging the holes.

. Introduction:

Today the illicit activities of the hackers are growing by leaps and bounds, viz., “THE RECENT ATTACK ON THE DNS SERVERS HAS CAUSED A LOT OF HULLABALOO ALL OVER THE WORLD”. However, fortunately, the antagonists reacted promptly and resurrected the Internet world from the brink of prostration.

Since the inception of conglomerating Computers with Networks the consequence of which shrunk the communication world,hitherto, umpteen ilks of security breaches took their origin. Tersely quoting some security ditherers – Eavesdropping, Hacking, Hijacking, Mapping, Packet Sniffing, 1Spoofing, DoS & DDoS attacks, etc. Newton’s law says “Every action has got an equal but opposite reaction”. So is the case with this. Nevertheless the security breaches and eavesdroppers, the technological prowess has been stupendously developed to defy against each of the assaults. Our paper covers the ADVANCED technical combats that have been devised all through the way, thus giving birth to the notion of **“NETWORK -SECURITY”.** Various antidotes that are in fact inextricable with security issues are – Cryptography, Authentication, Integrity and Non Repudiation, Key Distribution and certification, Access control by implementing Firewalls etc.

To satiate the flaws in the network security more and more advanced security notions are being devised day by day. Our paper covers a wide perspective of such arenas where the contemporary cyber world is revolving around viz.

Network security deals with the problems of legitimate messages being captured and replayed. Network security is the effort to create a secure computing platform. The action in question can be reduced to operations of access, modification and deletion. Many people pay great amounts of lip service to security but do not want to be bothered with it when it gets in their way. It’s important to build systems and networks in such a way that the user is not constantly reminded of the security system. Users who find security policies and systems to restrictive will find ways around them. It’s important to get their

feed back to understand what can be improved, the sorts of risks that are deemed unacceptable, and what has been done to minimize the organizations exposure to them. Network security problems can be divided roughly into four intertwined areas:

Secrecy, Authentication, Nonrepudation, and Integrity control.

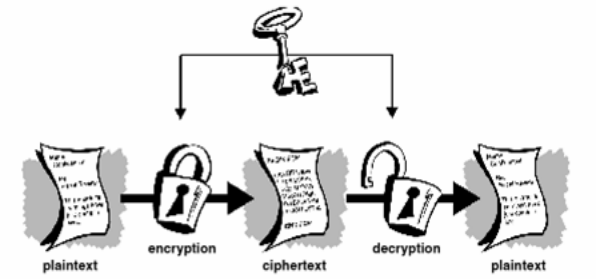
- **Secrecy** has to do with keeping information out of the hands of unauthorized users.
- **Authentication** deals with whom you are talking to before revealing sensitive information or entering into a business deal.
- **Nonrepudation** deals with signatures.
- **Integrity control** deals with long enterprises like banking, online networking.

These problems can be handled by using cryptography, which provides means and methods of converting data into unreadable from, so that valid User can access Information at the Destination.

Cryptography is the science of using mathematics to encrypt and decrypt data.

Cryptography enables you to store sensitive information or transmit it across insecure networks (like the internet)

So that it cannot be read by anyone expect the intended recipient. While cryptography is the science of securing data, cryptanalysts are also called attackers. Cryptology embraces both cryptography and cryptanalysis.



KEY PROCESSTECHNIQUES:

There are three key process techniques. They are:

- **Symmetric-key encryption**
- **A symmetric-key encryption**
- **Hash functions**

Symmetric-key encryption (one key):

There is only one key in this encryption. That is **private key.** This key is only used for both encryption and decryption. This is also called as **private-key encryption**. In this method the sender encrypt the data through private key and receiver decrypt that data through that key only.

Private Key method

Private Key method

Asymmetric-key encryption (two keys):

There are two keys in this encryption. They are:

- Public key
- Private key

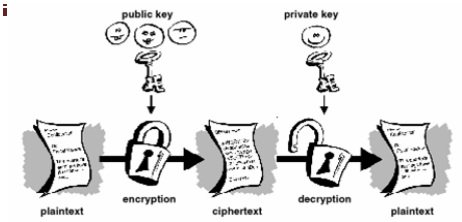
Two keys – a **public key** and a **private key,** which are mathematically related, are used in public-key encryption. To contrast it with symmetric-key encryption, public-key encryption is also some times called **public-key encryption**.

In public key can be passed openly between the parties or published in a public repository, but the related private key remains private. Data encrypted with the public key can be decrypted only using the private key. Data encrypted with the private key can be decrypted only using the public key. In the below figure, a sender has the receiver's public key and uses it to encrypt a message, but only the receiver has the related private key used to decrypt the message.

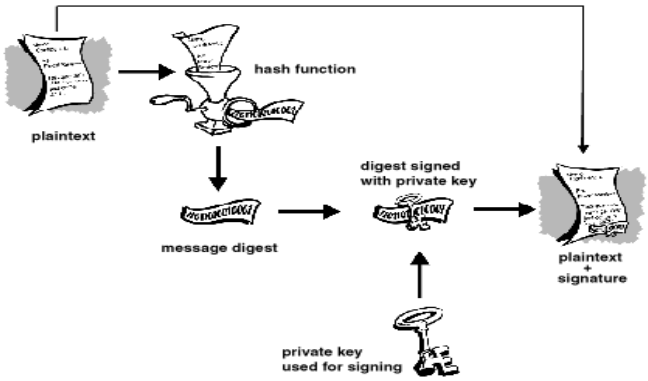
Public key method

Hash functions:

An improvement on the public key scheme is the addition of a one-way hash function in the process. A one-way hash function takes variable length input. In this case, a message of any length, even thousands or millions of bits and produces a fixed-length output; say, 160-bits. The function ensures that, if the information is changed in any way even by just one bit an entirely different output value is produced.



As long as a secure hash function is used, there is no way to take someone's signature from one documents and attach it to another, or to alter a signed message in any way. The slightest change in signed documents will cause the digital signature verification process to fail.



ADVANCED CRYPTOGRAPHIC TECHNIQUE

STEGANOGRAPHY

INTRODUCTION:

Over the past couple of year's Steganography has been the source of a lot of discussion. Steganography is one of the fundamental ways by which data can be kept confidential. Steganography hides the existence of a message by transmitting information through various carriers. Its goal is to prevent the detection of secret message.

Steganography uses techniques to communicate information in a way that is a hidden. The most common use of Steganography is hiding information, image or sound within the information of another file by using a **stegokey** such as password is additional information to further conceal a message.

There are many reasons why Srteganography is used, and is often used in significant fields. It can be used to communicate with complete freedom even under conditions that are censured or monitored.

The Steganography is an effective means of hiding data, there by protecting the data from unauthorized or unwanted viewing. But stego is simply one of many ways to protect confidentiality of data. Digital image steganography is growing in use and application. In areas where **cryptography** and strong **encryption** are being

outlawed, people are using steganography to avoid these policies and to send these messages secretly. Although steganography is become very popular in the near future.

WHAT IS STEGANOGRAPHY?

The word steganography comes from the Greek name "stegnos" (hidden or secret) and "graphy" (writing or drawing") and literally means hidden writing. Stegenography uses techniques to communicate information in a way that is hidden.

The most common use of Steganography is hiding information image or sound within the information of another file by using a **stegokey** such as password is additional information to further conceal a message.

WHAT IS STEGANOGRAPHY USED FOR?

Like many security tools, steganography can be used for variety of reasons, some good, some not so good. Steganography can also be used as a way to make a substitute for a one-way hash value. Further, Steganography can be used to tag notes to online images.

CRYPTOGRAPHIC TECHNOLOGIES

Based on layers:

- Link layer encryption
- Network layer encryption
- IPSEC, VPN, SKIP
- Transport layer
- SSL, PCT (private Communication Technology)
- Application layer
- PEM (Privacy Enhanced Mail)
- PGP (Pretty Good Privacy)
- SHTTP

Cryptographic process can be implemented at various at various layers starting from the link layer all the way up to the application layer. The most popular encryption scheme is SSL and it is implemented at the transport layer. If the encryption is done at the transport layer. If the encryption is done at the transport layer, any application that is running on the top of the transport layer can be protected.

Based on algorithms:

- **Secret-key encryption algorithms (symmetric algorithms)**
  - DES (Data Encryption Standard)—56bitkey
  - Triple DES—112bitkey
  - IDEA (International Data Encryption Algorithm)—128bitkey

- **Public-key encryption algorithms (Asymmetric algorithms)**

Diffie-Hellman (DH): Exponentiation is easy but computing discrete algorithms from the resulting value is practically impossible.

- **RSA:** Multiplication of two large prime numbers is easy but factoring the resulting product is practically impossible.

APPLICATIONS OF CRYPTOGRAPHY

- Defense service
- Secure Data Manipulation
- E-Commerce
- Business Transactions
- Internet Payment Systems
- Pass Phrasing Secure Internet Comm.
- User Identification Systems
- Access control
- Computational Security
- Secure access to Corp Data
- Data Security

APPLICATIONS OF NETWORK SECURITY

Computer networks were primarily used by university researchers for sending email, and by corporate employees for sharing printers. Under

these conditions, security did not get a lot of attention.

But now, as millions of ordinary citizens are using networks for:

- Banking
- Shopping
- Filling their tax returns

CONCLUSION:

Network security is a very difficult topic. Every one has a different idea of what "security" is, and what levels of risks are acceptable. The key for building a secure network is to define what security means to your organization. Once that has been defined, everything that goes on with. The network can be evaluated with respect to the policy. Projects and systems can then be broken down into their components, and it becomes much simpler to decide whether what is proposed will be conflict with your security policies and practices.

Security is everybody's business, and only with everyone's cooperation, intelligent policy, and consistent practices, will it be achievable.

Cryptography protects users by providing functionality for the encryption of data and authentication of other users. This technology lets the receiver of an electronic messages verify the sender, ensures that a message can be read only by the intended person, and assures the recipient that a message has not be altered in transmit. The Cryptography Attacking techniques like Cryptanalysis and Brute Force Attack. This paper provides information of Advance Cryptography Techniques.

BIBOLOGRAPHY:

- "Computer Networks ", by Andrew S.Tanunbaum
- "Fighting Steganography detection" by Fabian Hansmann
- "Network security" by Andrew S.Tanenbaum
- "Cryptography and Network Security" by William Stallings
- "Applied Cryptography" by Bruce Schneier, JohnWillley and Sons Inc
- URL: http://www.woodmann.com/fravia/fabian2.html.
- URL: http://www.jjtc.com/stegdoc/sec202.html.