Cryptography and Network Security

Prof. Miss. Sujata S. Khobragade
MCA Dept.
S.R.P.C.E.
Nagpur, India
sujatakhobragade.mca@gmail.com

Prof. Mr.Paritosh Sardare
MCA Dept.
S. R.P.C.E.
Nagpur, India
parisardare@gmail.com

Prof.Miss. Bhagyashri Kumbhare
MCA Dept.
S.R.P.C.E.
Nagpur, India
bha.kumbhare@gmail.com

Prof. Miss. Pallavi Dongre
MCA Dept.
S.R.P.C.E.
Nagpur, India
dongrepallavi5@gmail.com

Prof. Mr. Dipak Jha
IT Dept.
S.R.P.C.E.
Nagpur, India
dablu_jha135@yahoo.co.in

***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. 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 ilk of security breaches took their origin. Tersely quoting some security ditherers – Eavesdropping, Hacking, Hijacking, Mapping, Packet Sniffing, 1Spoofing, DoS & DDoS attacks, etc.**

This 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. This paper covers a wide perspective of such arenas where the contemporary cyber world is revolving around viz.

***Keywords*— Secrecy, Authentication, Non Repudiation and integrity control.**

INTRODUCTION

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, Non repudiation, 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.

•Non repudiation 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 PROCESS TECHNIQUE:

There are three key process techniques:

1) Symmetric key encryption

2) A Symmetric key encryption

3) HASH Function

SYMMETRIC KEY ENCRYPTION

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

A SYMMETRIC KEY ENCRYPTION

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 sometimes 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 FUNCTION

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 years 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 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 as tegokey such as password is additional information to further conceal a message. There are many reasons why Steganography 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, thereby 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 although steganography is become very popular in the near future.

WHAT IS STEGANOGRAPHY?

The word steganography comes from the Greek name “steganos” (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.

The advantage of steganography, over cryptography alone, is that messages do not attract attention to themselves. Plainly visible encrypted messages—no matter how unbreakable—will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal. Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties.

Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. As a simple example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.

STEGANOGRAPHY PROGRAM

There are several programs that can be used to hide data. This section will take a look at a couple of the more popular one on both Linux and Windows platforms. This is not a comprehensive list, but as a forensics expert, you should be familiar with the most popular programs in case you suspect steganographically hidden data in a file. You will find that many of the steganography programs available leave a fingerprint, thus providing you with a good starting point when attempting to reverse the steganographic process.

CAMOUFLAGE (Windows)

Camouflage is widely known as a good example of a steganographic program. it makes a simple job of inserting one file into another. The first sign that this program may not be the best choice for those who are serious about hiding data is that you can hide any type of file inside another. What this essentially means is that the hiding process is not dependent upon an individual file structure. Instead of hiding the data into a specific file type by flipping bits, over writing random pixels, or by some other explicit algorithm, Camouflage simply tags the encrypted file onto the end of the original file.

*JPHIDE (Windows and *nix)*

Jphide attempts to not only hide data, but also hide the fact that steganography is even in use. As illustrated by Camouflage, preventing detection of steganography is rule #1 when working with any steganographic program. After all, if an attacker can detect that steganography is in use, they can systematically attack it until they figure out what program was used in the steganographic process.

To understand how jphide works, it is necessary to dissect the structure of a jpeg. "Detecting Steganographic Content on the Internet" states, "The JPEG image format uses a discrete cosine transform (DCT) to transform successive 8_8-pixel blocks of the image into 64 DCT coefficients each. The least significant bits (LSB) of the quantized DCT coefficients are used as redundant bits into which the hidden message is embedded." In other words, each pixel block in a jpeg contains a small area that is basically worthless with regards to the image quality; however, this bit does provide a steganographer an excellent place to store data.

Unfortunately, if you simply start overwriting every insignificant bit of a DCT with data of your choice, you will create a mathematically/statistically noticeable fingerprint. The fingerprint becomes even more noticeable if you insert data into the LSB of each DCT and then simply stop when there is no more data. In this case, you will create a virtual cliff inside the jpeg that marks the end of the inserted data.

INVISIBLE SECRETS

One of the functions of Invisible Secrets is to hide files. Using a simple built in wizard, a file can be embedded in a JPEG, BMP, WAV, PNG or HTML file (figure Steg-8). While the hiding techniques are not too different than other LSB types of programs, Invisible Secrets attempts to hide the fact that steganography was used. With the exception of the HTML hiding, which is easy to spot because inserted text alters the standard '20' hex character used to represent blank space, Invisible Secrets does a fairly good job at hiding data. In addition, with a wide selection of encryption algorithms, any extracted information that is hidden in a file will have to be decrypted. Since the default encryption is AES 256, decryption is probably not likely.

STEGANOGRAPHY DETECTION

The simple rule of any steganography is that detection should not be possible. However, it is very difficult to hide data without leaving some type of trail or indicator behind. While some programs seems to make no effort at hiding the use of steganography but simply appending the 'hidden' data to the end of the file, other programs use clever algorithms that insert bits of data into host files at random locations using a random process. This section will take a look at several programs that focus on detecting the use of steganography.

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.

.html

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. Everyone 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, 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 and consistent practices, will it be achievable. Attacking techniques like Cryptanalysis and Brute Force Attack.

This paper provides information of Advance Cryptography technique.

References

[1] “Computer Networks”, by Andrew S.Tanunbaum
[2] “Fighting Steganography detection” by FabianHansmann
[3] “Network security” by Andrew S.Tanenbaum
[4] “Cryptography and Network Security” by William Stallings
[5] “Applied Cryptography” by Bruce Schneier, John Willley and Sons Inc
[6] “Information hiding techniques for stegnography and digital watermarking” by Petitcolas, Fabian A.P.; KatzenbeisserStefan(2000).
[7] URL:http://www.woodmann.com/fravia/fabian2.html.
[8] URL:http://www.jjtc.com/stegdoc/sec202.html.