Cryptography and Steganography: Security in Electronic Transactions

Angel O. Barbosa, Idelfonso Acevedo, Janneth Rodríguez and Abed Shehadeh
Engineering Management Graduate Program
Polytechnic University of Puerto Rico

Alfredo Cruz, PhD.
Associate Professor
Department of Electrical Engineering
Polytechnic University of Puerto Rico
alcruz@pupr.edu

ABSTRACT

A new use for two ancient arts and sciences; Cryptography and Steganography are now as useful as they were thousands of years ago. The digital communication security rests mainly on the developments of these two methodologies to assure that the flow of information generated by the e-commerce (e means electronic), the Internet, and other electronic transactions, require to be protected against unauthorized interventions. By developing and applying these techniques, the flow of information is kept under reasonable protection from outside unwanted intruders.

On the other hand, the governments of some countries around the world are considering to establish methods to control the use of these technologies. Meanwhile, there are groups that are against any intent of control or restriction from part of the Government for the use of these methods.

SINOPSIS

Un nuevo uso para un arte y una ciencia antiguas, la Criptografía y la Esteganografía son ahora tan útiles como lo fueron hace miles de años. La seguridad en la comunicación digital se apoya principalmente en el desarrollo de estas dos técnicas para asegurar el flujo de la información generada por el uso del comercio electrónico, el de la Internet, y otras transacciones electrónicas que requieren estar protegidas contra las intervenciones subrepticias. Al desarrollar y aplicar estas técnicas se logra mantener el flujo de información razonablemente protegido contra las intervenciones externas no deseadas .

Por otro lado, algunos gobiernos alrededor del mundo están considerando seriamente establecer reglamentaciones y leyes que controlen el uso de estas dos técnicas. Mientras tanto, existen grupos que están en contra de cualquier intento de control o restricción por parte del gobierno para la utilización de estos métodos.

I- INTRODUCTION

The present time is also known as the Communications Age, where the Internet has reduced the distance, the time required, the complexity, and the cost of communications around the world. Life styles have been impacted dramatically with the application of electronic transactions for most of our routine tasks. The e-mail, the e-commerce, the e-bank, ATM's, the chat rooms, and others terms are part of the daily life.

However, the methods of making transactions must offer a guaranty of confidentiality and fraud free environment to the user. The information that is sent, received or processed by digital means has to remain intact from the beginning to the end of the transaction. Intact means that the information has not been intercepted, reviewed, altered, handled, or in any way have been out of the control of the persons or entities originally intended or involved.

The unwanted, undetected, and unauthorized intervention from a third party is considered a violation to the privacy. The intrusions that can affect the information transmitted or its related systems are also known as attacks. The measures to control and to minimize these possibilities rely on the Cryptography and on the Steganography. Both terms come from the Greek: Cryptography from "Kruptos" (hidden), and Steganography from "Steganos" (covered or secret) and, for both, "graphos" (writing).

At some period during history, both terms were referred as equivalent. In the present time, they are considered as two techniques that are directed to the solution of a common problem. During WWII, both methods were used intensively by the nations in conflict. Messages were encrypted, so that the enemy could not obtain the information. Germans developed a steganographic technique known as the "microdots" that consisted in text and/or images that were extremely reduced in size as to fit in the point of the letter "i".

II- BASIC CONCEPTS AND DEFINITIONS

Today, in the Communications Age, each of these two technologies have a different approach for message handling. Cryptography pretends to cipher a message, so that it cannot be deciphered by any other than the party to whom the original message was intended. Steganography is focused into hiding or concealing the message in such a way that the existence of the message is not detected.

Cryptography covers two different ways of achieving its purpose. One way is the substitution method, in which the characters are ciphered by the substitution of other characters or symbols. The second method is obtained by transposing the positions of the characters in a predetermined order known only by the sender and the receiver. Steganography uses pictures, text, or audio media as the message carrier or "container" that embeds the secret message internally.

III- IMPORTANCE OF THE ELECTRONIC COMMUNICATION TECHNIQUES

Both, cryptography and steganography, help to provide integrity, accuracy, confidentiality, and verification to the transactions executed in electronic communications [1]. They are powerful tools against fraud, privacy violations, criminal attacks and electronic vandalism, and assure the validity of the transactions.

Security cannot be guaranteed 100% because intruders are always waiting for the opportunity to enter to look for the weaknesses of the encryption program and the encrypted message. But certainly, a confidence close to 100% can be achieved with these e-security methods.

IV- TYPES OF ATTACKS

There are different threats that always represent a real danger to the integrity of the messages sent through the system [2]. The following list covers some of these attacks [3]:

1- ***Ciphertext Only Attack*** - the attacker does not know anything about the contents of the message and works from the cipher text only. This attack bases its predictability on the information and the formats used.

2- ***Known Plaintext Attack*** - the attacker knows or can deduct part of the plaintext. This attack is based on anything about the contents of the message and works from the cipher text only. It bases its predictability on the information and the formats used.

3- ***Chosen Plaintext Attack*** - the attacker is capable of encrypting any text he likes with the unknown key.

4- ***Man - in - the - Middle Attack*** - this attack is related for cryptographic communication and key exchange protocols. In this attack, the intruder places himself between the sender and the receiver. Then, he interchanges his key with both sides so he is able to get the information. In this case, the sender and the receiver end up with a different key.

5- ***Correlation*** - in this attack, the main source of information is the correlation between the secret key and the output of the cryptosystem. By studying the correlation of the signals generated by the cryptosystem, sometimes the key is "leaked" from the cryptosystem. In other instances, the key is "guessed" based on the observed information.

6- ***Attacks against the hardware*** - this attack takes benefit from the data generated by the small cryptographic devices that perform encryptions. Once it gets the information, this is analyzed and related in order to break the key .

V- TYPES OF CRYPTOGRAPHY

Cryptography can be classified in three different types according to the characteristics of how the keys are combined in order to obtain the security level [4].

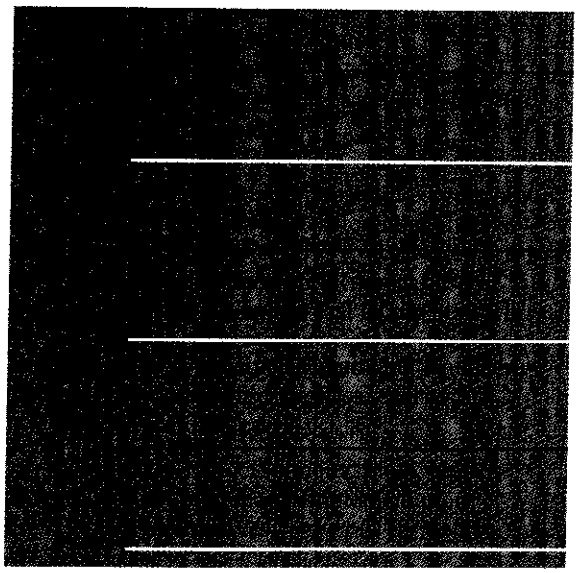
A. Symmetric Cryptography

In the symmetric cryptosystems, the same key (the secret key) is used to encrypt and decrypt a message. In other words, both, the sender and the receiver, use the same key. A problem of the symmetric cryptosystem is how to keep the secrecy of the key that is sent through the same channels that are being observed by the intruders.

The message is encrypted using algorithms. The most popular algorithms to encrypt messages is called as DES (Data Encryption Standard); this algorithm has been attacked successfully by the crypto-analysts. As the result of the weakness of DES, the NIST (National Institute of Standards and Technology) has requested proposals for an official successor that meets

the present and future requirements. AES (Advanced Encryption Standard) will be the name of this successor. This algorithm will be required to has a symmetric block cipher, a variable key size able to work with 128 bits block size, and supporting 128, 192 and 256 bit keys. The Table 1 summarizes the algorithms considered for AES [4].

***Table 1**: AES algorithms under consideration for year 2001*



B- Asymmetric Cryptography

The asymmetric cryptosystems use the public key to encrypt the message and a different key, or private key, to decrypt it [5]. This technique is used mainly by banks and in the e-commerce. Examples of asymmetric algorithms are: 1) ELGAMAL Diffie-Hellman 1976. It is 1,000 to 10,000 times slower than a symmetric key algorithms. It has uses in authentication and digital signatures. 2) RSA Rivest, Shamir, Adleman 1978. The RSA algorithm can be represented with the following formulas:

To encrypt the message;

$$C = M^e \pmod n$$

To decrypt the message;

$$M = C^d \pmod n$$

where;

C = ciphered message
M = message
e = an altern prime number lower than the module
n = the module
d = a predetermined value

C- Hybrid System Cryptography

Hybrid systems are the result of the need to transmit big amounts of data at an acceptable speed in a safe manner. Those systems use symmetric and asymmetric key cryptography. In addition, this type of cryptography has some limitations or disadvantages: any of the parties can be substituted and they require certifications provided by the responsible authorities that includes the name, the expedition and expiration dates. The Diffie-Hellmann Algorithm allows that two users interchange one key through the Internet.

VI- CRYPTOGRAPHIC PROTOCOLS AND STANDARDS

Cryptography works on many levels. The first level is the algorithm like block ciphers and public key cryptosystem. These are used to build protocols, and protocols are used to build applications or other protocols.

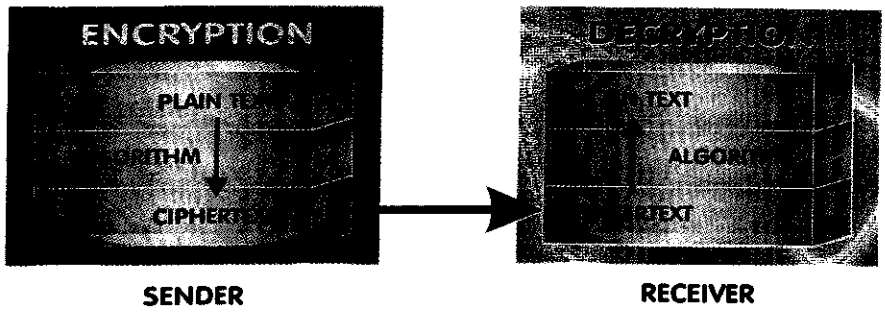


***Figure 1:** Symmetric cryptography: plain text is encrypted and decrypted with the same algorithm.*

It is important to consider the big picture when working with the applications. In order to have a secure system, the algorithm, the protocol, and the application have to be strong and leak proof. As an example, if a good and secure algorithm is used in a protocol, and this protocol is not strong enough and leaks information, then the system is weak. This rational is also valid for the applications. The following are well known protocols and standards:

1– ***Domain Name Server Security (DNSSEC)*** - This is a protocol for secure distributed name services.

2– ***Generic Security Services API (GSSAPI)*** - This provides authentication, key exchange and encryption interface to different algorithms and systems.

3– ***Secure Socket Layer (SSL)*** - This is one of the two protocols used for secure www connections. It is important because of the increase of sensitive information transmitted through the Internet.

4– ***Secure Hypertext Transfer Protocol (SHTTP)***- This is the other protocol used in www. It is more flexible than SSL.

5– ***E-Mail Security and Related Services*** - Open PGP is a standardization of the Original PGP developed by Phil Zimmerman. It has become a standard.

6– ***Publius Censor-Resistant Publishing Protocol***- This is a very advanced system that allows a group of authors and readers to share documents on a set of web servers without revealing or leaking the identity. Documents are certified to come from a certain, pseudonymous author and cannot be removed or modified, unless a large amount of the involved web servers are compromised.

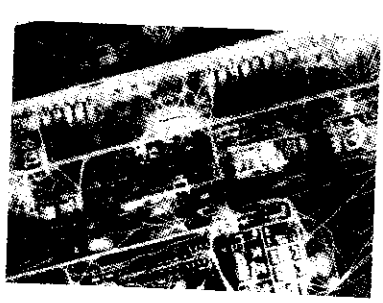
7– ***Public Key Encryption Standards (PKCS)***- Standards developed by RSA Data Security. It defines safe ways of use of the RSA.

8– ***IEEE1363 - Standard Specification Public Key*** - This is an upcoming standard for public key cryptography. Consists of several public key algorithms for encryption and digital signatures.

9– ***SSH2 Protocol*** - Is developed by IETF Working Group. A very versatile protocol for the needs of the internet.

All the previous protocols operate on the application layer of the Internet, allowing particular

(a) *(b)*



(c)

Figure 2: *(**a**) is the original picture from Renoir, (**b**) is the same picture with the embedded photography shown in (**c**), this picture correspond to a soviet air base taken by an American spy plane in 1960's.*

programs to communicate in a secure channel in an inherently insecure network. The next one works in the inherent security of the Internet system.

10– ***IPSEC***- Its purpose is to make the Internet secure in its essence.

VII- TYPES OF STEGANOGRAPHY

Steganography is the technique that hides a message inside another message [6]. It is based on two principles: 1) digital images or videos can be modified without changing the functionality of the carrier message, and, 2) humans cannot differentiate minute changes in colors and in sound quality. Some of the carriers ("containers") used in steganography are images, audio files, and diskettes or other media. The carrier is embedded with the information or message that is intended to be hidden. Authors of software recommend the use of encryption before embedding the image into the "carrier". The following formula represents the steganographic process:

Stego Media = Media Carrier + Hidden Message + Secret Key

A- Image and Audio

Programs based on algorithms to change the Least Significant Bit (LSB) of the pixel or the sound word. They do not produce any noticeable change in the image color or sound quality. Figure 2a is the container or carrier. Airfield photograph in Figure 2c is the message that was sent. Figure 2b shows the combination of the carrier embedded with the message [7]. Usually, the files related to images are in GIF, BMP, and JPEG formats. For audio are the WAV and MP3 file formats. These files have a very large capacity to conceal a message. The container size will depend on the size of the hidden file and the software used to cover the message. For example of image files, a common size of an image is 640 X 480 pixels and 256 colors. If each pixel is defined with eight (8) bits, by using only the Least Significant Bit (LSB), there will be 300Kbits available to hide the message. The software used to perform the hiding is a factor that may affect the available capacity to perform the covering.

B- Floppy Disks, CD's

In this method, the message is hidden in the empty sectors of the disks without affecting the original data saved in those disks.

C- File Compression - Effects

The integrity of the message can be affected depending on the type of compression used. There are two types of compression: lossless and lossy. The integrity of the information is kept by using lossless compression. On the other hand, the use of lossy compression can introduce changes to the message sent.

D- Image Softwares

The following softwares are used for steganographic applications:

1– ***Hide and Seek v4.1 and 5.0*** - Hide and Seek v4.1 is a free software that contains several DOS programs that can place data in GIF files. This software has limitations with the minimum and maximum sizes that it can handle. If the image is smaller than the minimum required for the message, then the image is filled out with black space. This software uses the LSB of each pixel. The larger the image, the highest the tendency of image degrading.

2– ***StegoDOS or Blackwolf's Picture Encoder v.0.90a.*** - This is a public domain software consisting of several DOS programs. It requires too much effort for the obtained results. It only works with images with 320 X 200 and 256 colors.

3– ***White Noise Storm (WNS)*** - It is a very good tool for DOS. It is easy to use and it does not introduce any noticeable degrading of the image after inserting the message. This method uses the Least Significant Bit less successfully than other software. It incorporates an EOF bit that indicates the presence of a message. When a message is removed, it is found with garbage at the end. A major disadvantage is the loss of many bits that, otherwise, could be used for data storage.

4– ***Steganographic Tools For Windows 3.0*** - A very good tool. It includes several programs to process GIF and BMP for images, WAV for audio, and FDD that is used in diskettes.

E- Other Uses: Digital Watermarking

These are techniques that create and embed invisible digital marks in image and audio files [8]. In modern communications it is very easy to copy

documents from other persons and present them as original. By using appropriate programs, invisible marks containing information of copyright, name, address, etc., are created. This is very useful for artists, authors, and owner of intellectual property. By using algorithm based programs, it can be determined when the information is copied or reproduced without authorization. Digital Watermarking can be used in several applications, such as:

1– ***Copyright Protection of Digital Media*** - Identify names and addresses of authors and owners of the data.

2– ***Data Security*** - Provides certification, authentication and conditional access in I.D. cards, passports, etc. Detects alteration or modification to prevent malicious tampering of private and confidential documents like company memos, e-mails and letters.

3– ***Copy Controls*** - To prevent the use of illegal software copies.

4– ***Industrial Uses*** - May be used as a geometrical reference for programs as Optical Character Recognition (OCR).

VIII- REGULATIONS AND CONTROLS

The same data scrambling and hiding technology that allows to send the credit card number across the Internet, also makes harder to the law enforcement authorities to detect a terrorist plot or a criminal action.

Law enforcement agencies cannot decipher the messages encrypted with the recent developed software. These new products are so powerful that even with massive supercomputers they are not successful in breaking the key. This is a common situation in other countries of the world.

Until 1996, the United States Government considered that anything stronger than a 40 bits encryption was considered a "munition", and it was illegal to export it. Now, 56 bit cryptography is allowed, but with some restrictions. Cryptography with 128 bits is already emerging as the new standard. The actual situation is creating a controversy in regards of the control of the keys of the system. Some Government officials support the idea that the key has to be given to the Government, and under certain circumstances, with a court order, this key can be used. The FBI director, Louis Freech and the Attorney General, Janet Reno are behind this approach.

There is another group composed mainly by US software companies that are against any intent of establishing restrictions. If the restriction are approved, the ability of these companies to compete internationally will be affected.

Before 1991 only the Government and the large corporations used the encryption technology. In 1993, Phil Zimmerman developed PGP. This software was based on 128 bit encryption. Soon, the software was available in other countries and he was submitted to a criminal investigation. In 1993, the Clinton administration proposed a government designed encryption called the "Clipper Chip" to be used as the industry standard. The proposal was not accepted. In 1996, President Clinton declared that encryption would no longer be considered a munition, unless it was created specifically for military purposes.

IX- CONCLUSION

Cryptography is an essential part of today's information systems. It provides accountability, fairness, accuracy and confidentiality to the transactions. It prevents fraud in the e-commerce and assure the validity of the financial transactions, it can prove the identity or it can protect the anonymity, it keeps vandals from altering your web page, it prevents the industrial spies from obtaining corporate information, it keeps your personal records confidential.

Cryptography is moving to provide more security in electronic transactions. Steganography will provide the security techniques that are required in the management of information flow. Steganography has evolved and is continuing to receive the attention from the academic and the industrial communities. As an example, there is a patent pending for a lossless steganographic algorithm that does not affect the data integrity of the container file, and the program is completely independent of the size of the "container" file relative to the hidden file.

In the future, Cryptography and Steganography will move to be a complement one to the other [9].

X- REFERENCES

[1] Francis Litterio, "The Study of Encryption", *http//world.std.com/~franl/crypto.html*

[2] SSH-Tech Corner, "Introduction to Cryptography", *http://www.ssh.fi/tech/crypto/intro.htm*

[3] Monjas M.A., Criptozona, http://www.dat.etsit.upm.es/~mmonjas/cripto/

[4] B. Schneier, "Why Cryptography is Harder Than It Looks," *http:// www.counterpane.com/whycrypto.html/*

[5] SSH – Tech Corner, "Cryptographic Algorithms", *http://www.ssh.fi/tech/crypto/algorithms.html/*

[6] Neil F. Johnson, "Steganography", 1995-2000 *http://www.jjtc.com/stegdoc/.*

[7] Neil F. Johnson, "Steganography", 1995-2000 *http://www.jjtc.com/stegdoc/*

[8] Alp Vision, "Digital Watermarking", *http://www.alpvision.com/watermarking.html/*

[9] Johnson N.F., "Steganography", *http://www.jitc.com/stegdoc/*

XI- OTHER USEFUL REFERENCES

[1] Introduction to Cryptography http://www.ssh.fi/tech/crypto/intro.html/

[2] McBride Baker&Coles, "Summary Of E-Commerce and Digital Signature Legislation", http://*www.mbc.com/ecommerce.html/*

[3] Anthony T.S. Ho, Siu-Chung Tam, Siong-Chai Tan and Lian-Teck Yap, "Digital Steganography for information security" http://*www.datamark-tech.com/*

[4] Froomkin D., "Deciphering Encryption" http://www.washingtonpost.com/wpsrv/politics/special/encryption/encryption.httm/

[5] Anderson Ross, "Analysis and design of cryptographic algorithms. http://www.cl.cam.ac.uk/users/rja114/