International Journal of Information Technology and Knowledge Management
July-December 2011, Volume 4, No. 2, pp. 515-517

CHAFFING AND WINNOWING WITHOUT USING STEGANOGRAPHY AND ENCRYPTION TECHNIQUE

Amitabh Maurya[1], Pankaj Kumar Saini[2] & Navnish Goel[3]

Steganography is the art of concealing the existence of information and hiding information of embedded information. Steganography can be viewed as akin to cryptography. Both have been used throughout recorded history as means to protect information. At that time these two technologies seem to converge while the objectives of the two differ. Cryptographic techniques "scramble" messages so if intercepted, the messages cannot be understood. Steganography, in an essence, "camouflages" a message to hide its existence and make it seem "invisible" thus concealing the fact that a message is being sent all together. An encrypted message may draw suspicion while a visible message will not. In this paper we will discuss how to achieve confidentiality without using encryption when sending data over an insecure channel. The name is derived from agriculture: after grain has been harvested and threshed, it remains mixed together with inedible fibrous chaff. This technique is remarkable compared to ordinary encryption methods because it allows the sender to deny responsibility for encrypting their message. This paper also analyses the performance of some of the Steganography tools. Steganography is a useful tool that allows covert transmission of information over the communications channel. This paper will take an in-depth look at this technology by introducing the reader to various concepts of Cryptography, a brief history of Steganography and a look at some of the Steganography technique.

Keywords: Steganography, Encryption, Cryptography, Variations, Null Cipher.

1. Introduction

A major goal of security techniques is "confidentiality"—ensuring that adversaries gain no intelligence from a transmitted message. There are two major techniques for achieving confidentiality:

1.1 Steganography

The art of hiding a secret message within a larger one in such a way that the adversary cannot discern the presence or contents of the hidden message. For example, a message might be hidden within a picture by changing the low-order pixel bits to be the message bits.

Steganography is derived from the Greek for covered writing and essentially means "to hide in plain sight". As defined by Caching [1] Steganography is the art and science of communicating in such a way that the presence of a message cannot be detected. Simple Steganography techniques have been in use for hundreds of years, but with the increasing use of files in an electronic format new technique for information hiding have become possible.

This document will examine some early examples of Steganography and the general principles behind its usage. We will then look at why it has become such an important issue in recent years. There will then be a discussion of some specific techniques for hiding information in a variety of files and the attacks that may be used to bypass Steganography.

Figure 1 shows how information hiding can be broken down into different areas. Steganography can be used to hide a message intended for later retrieval by a specific individual or group. In this case the aim is to prevent the message being detected by any other party. The other major area of Steganography is copyright marking, where the message to be Inserted is used to assert copyright over a document. This can be further divided into watermarking and fingerprinting which will be discussed later.

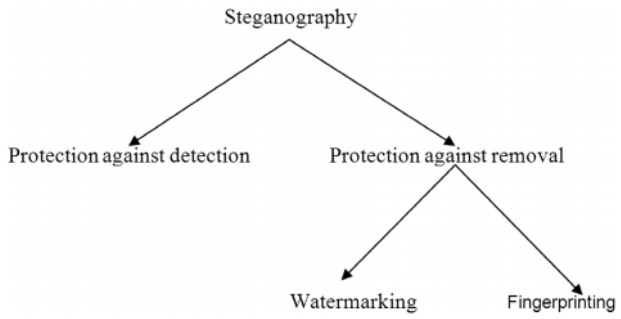

Fig.1: Types of Steganography

1.2 Encryption

Transforming the message to a cipher text such that an adversary who overhears the cipher text cannot determine the message sent. The legitimate receiver possesses a secret

[1, 2]Assistant Professors in Vidya College of Engineering Meerut (UP)
[3]Assistant Professors in S.D.College of Engineering and Technology, Muzaffarnagar (UP)
E-mail: [1]amit.maurya20@gmail.com

decryption key that allows him to reverse the encryption transformation and retrieve the message. The sender may have used the same key to encrypt the message or used a different, but related key (with public-key schemes). DES and RSA are familiar examples of encryption schemes. This paper introduces a new technique, which we call "chaffing and winnowing"— to winnow is to "separate out or eliminate" and is often used when referring to the process of separating grain from chaff.

2. STEGANOGRAPHY AND CRYPTOGRAPHY

2.1 Comparison of Steganography and Cryptography

Steganography and cryptography are closely related. Cryptography scrambles messages so it can't be understood. Steganography on the other hand, hide the message so there is no knowledge of the existence of the message. With cryptography, comparison is made between portions of the plaintext and portions of the cipher text. In Steganography, comparisons may be made between the cover-media, the stego-media, and possible portions of the message. The end result in cryptography is the cipher text, while the end result in Steganography is the stego-media. The message in Steganography may or may not be encrypted. If it is encrypted then a cryptanalysis technique is applied to extract the message.

2.2 Combination of Steganography and Cryptography

Those who seek the ultimate in private communication can combine encryption and Steganography. Encrypted data is more difficult to differentiate from naturally occurring phenomena than plain text is in the carrier medium. There are several tools by which we can encrypt data before hiding it in the chosen medium. In some situations, sending an encrypted message will across suspicion while an invisible message will not do so. Both methods can be combined to produce better protection of the message. In case, when the Steganography fails and the message can be detected, it is still of no use as it is encrypted using cryptography techniques.

3. CHAFFING AND WINNOWING

Chaffing and winnowing is a cryptographic technique to achieve confidentiality without using encryption when sending data over an insecure channel. The name is derived from agriculture: after grain has been harvested and threshed, it remains mixed together with inedible fibrous chaff. The chaff and grain are then separated by winnowing, and the chaff is discarded. The technique was conceived by Ron Rivest. Although it bears similarities to both traditional encryption and Steganography, it cannot be classified under either category.

This technique is remarkable compared to ordinary encryption methods because it allows the sender to deny responsibility for encrypting their message. When using chaffing and winnowing, the sender transmits the message unencrypted, in clear text. Although the sender and the receiver share a secret key, they use it only for authentication. However, a third party can make their communication confidential by simultaneously sending specially crafted messages through the same channel.

How it Work

The sender (A) wants to send a message to the receiver (B). In the simplest setup, sender enumerates the bits in the message and sends out each bit in a separate packet. Each packet contains the bit's serial number in the message, the bit itself, and a message authentication code (MAC) whose secret key A shares with B. C who transmits A's packets to B, interleaves the packets with corresponding bogus packets (called "chaff") with corresponding serial numbers, the bits inverted, and a random number in place of the MAC. C does not need to know the key to do that. B uses the MAC to find the authentic messages and drops the "chaff" messages. This process is called "winnowing". An eavesdropper located between A and C, can easily read A's message. But an eavesdropper between C and B would have to tell which packets are bogus and which are real (i.e., to winnow). That is infeasible if the MAC used is secure and C does not leak any information on packet authenticity. Example for whole process of chaffing and winnowing shown below.

Message	Authentication Using MAC and Secret Key		
	Serial Number	Data	MAC
Hi babloo	1	Hi babloo	30cd0e4
Meet me at	2	meet me at	24cm1f5
7pm	3	7pm	12fj3g6
At my home	4	At my home	34gfg49
Love Amitabh	5	Love Amitabh	31abc01

Transmitted Packets		MAC Checking by Receiver		
1	Hi babloo	30cd0e4	1	valid
1	Hi babloo	ue0123f	1	Invalid
2	meet me at	24cm1f5	2	valid
2	I'll meet you	24cm1f5	2	Invalid
3	7am	12fj36g	3	Invalid
3	7pm	12fj3g6	3	valid
4	At my home	34gfg49	4	valid
4	At my street	34gfg39	4	Invalid
5	Love Navnish	abc3101	5	invalid
5	Love Amitabh	31abc01	5	valid

Message Reconstruction Serial Number		Message Data
1.	Hi babloo	Hi babloo
2.	meet me at	meet me at
3.	7pm	7pm
4.	At my home	At my home
5.	Love Amitabh	Love Amitabh

4. VARIATIONS

The simple variant of the chaffing and winnowing technique described above adds many bits of overhead per bit of original message. To make the transmission more efficient, A can process her message with an all-or-nothing transform and then send it out in much larger chunks. The chaff packets will have to be modified accordingly. Because the original message can be reconstructed only by knowing all of its chunks, C needs to send only enough chaff packets to make finding the correct combination of packets computationally infeasible.

Chaffing and winnowing lends itself especially well to use in packet-switched network environments such as the Internet, where each message is sent in a separate network packet. In another variant of the technique, C carefully interleaves packets coming from multiple senders. That eliminates the need for C to generate and inject bogus packets in the communication. However, the text of A's message cannot be well protected from other parties who are communicating via C at the same time. This variant also helps protect against information leakage and traffic analysis.

4.1. Null Cipher

A null cipher is an ancient form of encryption where the plaintext is mixed with a large amount of non-cipher material. It would today be regarded as a simple form of Steganography. Null ciphers can also be used to hide cipher text, as part of a more complex system. In classical cryptography a null is intended to confuse the cryptanalyst. Typically, a null will be a character which decrypts to obvious nonsense at the end of an otherwise intelligible phrase. In a null cipher, most of the characters may be nulls.

An example follows: Tonight increasing snow. Unexpected precipitation smothers eastern towns. Be extremely cautious and use snow tires especially heading east. The knowingly slippery, highway evacuation is suspected. Police report emergency situations in downtown ending near Tuesday. In modern cryptology, null cipher (or NONE cipher) is also defined as choosing not to use encryption in a system where various encryption options are offered, such as for testing/debugging, or authentication-only communication.

4.2 E-mail Spam

E-mail spam, also known as junk e-mail or unsolicited bulk e-mail (UBE), is a subset of spam that involves nearly identical messages sent to numerous recipients by e-mail. Definitions of spam usually include the aspects that e-mail is unsolicited and sent in bulk. One subset of UBE is UCE (unsolicited commercial e-mail).E-mail spam has steadily grown since the early 1990s. Botnets, networks of virus-infected computers, are used to send about 80% of spam. Since the cost of the spam is borne mostly by the recipient, it is effectively postage due advertising. The legal status of spam varies from one jurisdiction to another. In the United States, spam was declared to be legal by the CAN-SPAM Act of 2003 provided the message adheres to certain specifications. ISPs have attempted to recover the cost of spam through lawsuits against spammers, although they have been mostly unsuccessful in collecting damages despite winning in court.

5. CONCLUSION AND FUTURE SCOPE

We have introduced a new technique for confidentiality, called "chaffing and winnowing". This technique can provide excellent confidentiality of message contents without involving encryption or Steganography. As a consequence of the existence of chaffing and winnowing, one can argue that attempts by law enforcement to regulate confidentiality by regulating encryption must fail, as confidentiality can be obtained effectively without encryption and even sometimes without the desire for confidentiality by the two communicants. Law enforcement would have to seek access to all authentication keys as well, a truly frightening prospect. Mandating government access to all communications is not a viable alternative. The cryptography debate should proceed by mutual education and voluntary actions only.

REFERENCES

[1] Ahsan K., and Kundur D., "Practical Internet Steganography: Data Hiding in IP" Found online at http://www.ece.tamu.edu~deepa/pdf/txsecwrksh03.pdf.

[2] A.Kumar.,and km.pooja., "Steganography- A Data Hiding Technique", Found Online at www.ijcaonline.org/archives/9/number7/1398-1887

[3] Ron Rivest., "Chaffing and Winnowing-MIT" people. csail. mit.edu/rivest/Chaffing.txt

[4] Fabien A.P., and Petitcolas, "Information Hiding: Techniques for Stegano[10] Digital Watermarking for Digital Media", Information Science Publishing.

[5] Hiding in Plain Sight: "Steganography and the Art of Covert Communication Cole", Eric.

[6] Information Hiding: "Steganography and Watermarking Attacks and Countermeasures", (Advances in Information Security, 1) Johnson, Neil F. / Doric, Zoran / Jajodia.

[7] Computerworld. Steganography: Hidden Data. "Quick Study by Deborah Radcliff", [Online] 2002. http://www.computerworld.com/securitytopics/security/story/0,10801,71726,00. html.