ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

An overview of advanced network protocol steganography

Ms. Dhanashri D. Dhobale [1], Dr.Vijay R. Ghorpade[2]

Assistant Professor, Information Technology, PVPIT, Budhgaon, Sangli, India [1]

Principal and Professor, Computer Science & Engg., DYPCOE, Kolhapur, India [2]

Abstract: Steganographic techniques have been used for ages and they date back to ancient Greece. The aim of steganographic communication back then and now, in modern applications, is the same: to hide secret data (a steganogram) in an innocently looking cover and send it to the proper recipient who is aware of the information hiding procedure. In an ideal situation the existence of hidden communication cannot be detected by third parties. What distinguishes historical steganographic methods from the modern ones is, in fact, only the form of the cover (carrier) for secret data. Historical methods relied on physical steganography – the employed media were: human skin, game, etc. Further advances in hiding communication based on the use of more complex covers, e.g. with the aid of ordinary objects, whose orientation was assigned meaning. This is how steganograms were introduced. The popularization of the written word and the increasing literacy among people had brought about methods which utilized text as carrier. Here we are giving the overview of network steganography history, evolution, principles, concepts and detection.

The World Wars had accelerated the development of steganography by introducing a new carrier – the electromagnetic waves. Presently, the most popular carriers include digital images, audio and video files and communication protocols. The latter may apply to network protocols as well as any other communication protocol (e.g. cryptographic).The way that people communicate evolved over ages and so did steganographic methods. At the same time, the general principles remained unchanged.

Keywords: Steganography, Network security, information hiding

1. INTRODUCTION

Steganography is a general term referring to all methods for the embedding of additional content into some form of carrier The choice of the carrier is nearly unlimited; it may be an ancient piece of parchment, as well as a network protocol header. Present day steganographic methods are far more sophisticated than their ancient predecessors, but the main principles had remained unchanged. They typically rely on the utilization of digital media files or network protocols as a carrier, in which secret data is embedded. Steganography is a general term referring to all methods for the embedding of additional secret content into some form of carrier, with the aim of concealment of the introduced alterations. The choice of the carrier is nearly unlimited; it may be an ancient piece of parchment, as well as a network protocol header. Inspired by biological phenomena, adopted by man in the ancient times, it has been developed over the ages. Present day steganographic methods are far more sophisticated than their ancient predecessors, but the main principles have remained unchanged. They typically rely on the utilization of digital media files or network protocols as a carrier, in which secret data is embedded. This paper presents the evolution of the hidden data carrier from the ancient times till the present day and pinpoints the observed development trends, with special emphasis on network steganography.

It can be concluded that steganography is becoming the new black among Black Hats. Let us take a closer look at the evolution of technique, with special attention directed towards the class of methods falling in the category of network steganography.

2. *MLS (Multi-Level Steganography):*

MLS is a new method of hiding communication in telecommunication network that uses features of an existing steganographic method (the upper-level method) to create a new one (the lower-level method). This is based on combining two or more steganographic methods in such a way that one method (the upper-level) is a carrier for the other method (the lower-level). From such a binding of information hiding solutions comes some interesting benefits, among others: Increased undetectability of upper-level methods, Increased total steganographic bandwidth, Ability to verify the steganograms integrity after its reception, Limiting the chance of successful steganogram extracting and reading.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

The idea of a simple two-method MLS, i.e., in which two steganographic methods are utilized as described above, and its comparison to the typical single network steganography method is presented in Fig. 1.

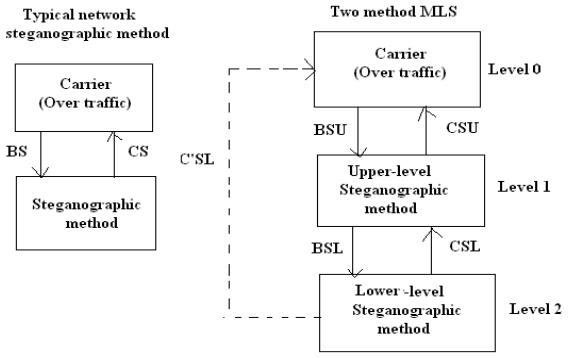

Fig. 1 The typical network steganography method (left) and the two-method MLS (right) comparison

In typical single-method network steganography, overt communication traffic is used as a carrier for secret data. By influencing the carrier, a certain steganographic bandwidth (BS), which is defined as the amount of the steganogram transmitted using a particular method in one second ([b/s]), is achieved. How-ever, the utilization of BS may result in a certain steganographic cost (CS) that expresses an impact (degradation) of a hidden data carrier due to steganographic procedure operations. The higher BS for given steganographic method we want to utilize the higher CS (the steganographic method has a greater impact on a hidden data carrier). If CS is excessive, then the detection of the method can be straight-forward.

Thus, a trade-off between BS and CS is always necessary. MLS is based on at least two steganographic methods. First, the upper-level method uses overt traffic as a secret data carrier. The second, the lower-level method, uses the way the upper-level method operates as a carrier. The indirect carriers for lower-level methods are still packets from overt communication, but the direct carrier is another (upper-level) method. For the MLS case presented in Fig. 1, the upper-level method affects the carrier by introducing a certain cost CSU, and under this circumstance, it achieves BSU. The lower-level method relies on the upper-level one for its steganographic bandwidth BSL For this reason, the lower-level method can influence the upper-level one by introducing a cost CSL but also the overt communication by introducing a cost C'SL. The cost C'SL depends on the choice of the lower-level method and, in particular, lower-level method can have no influence on the carrier i.e. it introduces no cost (C'SL ≈0).

3. HICCUPS: Hidden Communication System for Corrupted Networks:

HICCUPS (HIdden Communication system for CorrUPted networkS), a steganographic system dedicated to shared medium networks including wireless local area networks. The novelty of HICCUPS is: usage of secure telecommunications network armed with cryptographic mechanisms to provide steganographic system and proposal of new protocol with bandwidth allocation based on corrupted frames. The system presented takes advantage of imperfections of transmission medium environment – interferences and noise in communication medium – natural susceptibility to data distortion. HICCUPS is a steganographic system with bandwidth allocation for shared medium networks. We are aware that wired shared medium networks based on broadcast communication are rare nowadays as practically all new home and office networks use switches rather than hubs [7] (note: that is why new LANs based on switches are called switched networks). On the other hand all wireless local area networks do use and will use broadcast technique to communicate. Usage of wireless technology has rapidly grown in the last few years [6], making presented system applicable in practice. Wireless networks are much more susceptible to data distortion [8] than wired ones, therefore utilization of interferences and noise in communication medium in our system's performance seems to be much attractive.

The system is destined to be implemented in a network environment with the following three properties:

P1: shared medium network with possibility of frame's interception,

P2: publicly known method of cipher initiation for instance by initialization vectors,

P3: integrity mechanisms for encrypted frames for instance one-way hash function,

Cyclic Redundancy Code – CRC (note: CRC is rarely strong enough for protecting integrity, but it is used in IEEE 802.11 for such purpose [9]. The essential condition for HICCUPS is only P1 property – others are optional. There is no difference between the integrity mechanism for encrypted frames and integrity for other ones in some networks with P3 property.

It is possible to create three hidden data channels in MAC frame (Fig. 2) in networks that meets P1-P3 properties:

HDC1: channel based on cipher's initialization vectors,

HDC2: channel based on MAC network addresses (for example destination and source),

HDC3: channel based on integrity mechanism values (for example frame checksums).

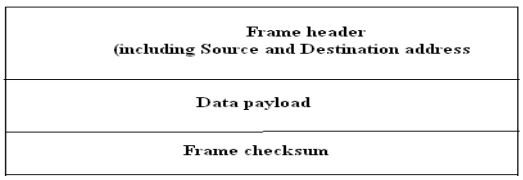

Fig. 2: Generic MAC frame

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

For network with property limited to P1 – network with no security applied or enabled – only HDC2 and HDC3 are used. Most of wired networks have no support for security at MAC layer as opposed to wireless. General HICCUPS operation scheme (Fig. 3) Is based on three modes: system initialization, basic mode, corrupted frame mode.

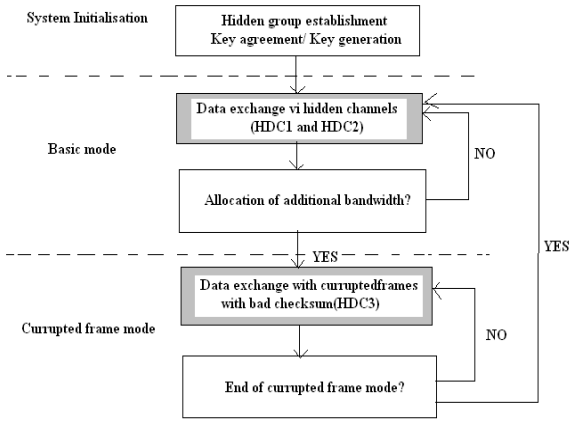

Fig.3: General HICCUPS operation scheme

In system initialization – all stations included in hidden group) establish secret key for ciphers embedded in steganographic system.

Basic mode of HICCUPS operation is data exchange based on cipher's initialization vectors (HDC1) and MAC network addresses (HDC2). For set sequence exchanged via HDC1 or HDC2 hidden group stations move in corrupted frame mode – mode with additional bandwidth.

In corrupted frame mode information is exchanged in data payload of frames with intentionally created bad checksums (HDC3). This mode offers almost 100% of bandwidth for a certain period.

4. LACK (Lost Audio Packets Steganography)

LACK is a hybrid intra-protocol steganographic method which modifies voice packets' time relations and their content. At the transmitter, some selected audio packets are intentionally delayed before transmitting. If the delay of such packets at the receiver is considered excessive, the packets are discarded by a receiver which is not aware of the steganographic procedure. The payload of the intentionally delayed packets is used to transmit secret information to receivers aware of the procedure, so no extra packets are generated. For unaware receivers the hidden data is "invisible".

5. RSTEG (Retransmission Steganography)

RSTEG is an intra-protocol hybrid network steganography method. It is intended for a broad class of protocols that utilizes retransmission mechanisms. The main innovation of RSTEG is to not acknowledge a successfully received packet in order to intentionally invoke retransmission. The retransmitted packet carries a steganogram instead of user data in the payload field. Fig 4 shows the generic retransmission scenario in left side and right side shows RSTEG using time outs.

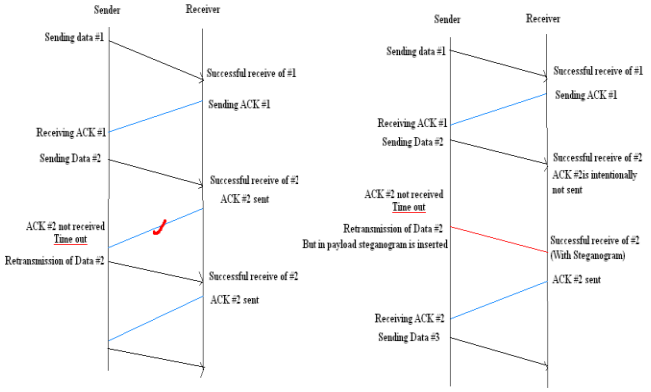

Fig. 4 Generic Retransmission using time out(Left) and using RSTEG(Right)

The RSTEG may be applied to the retransmission mechanisms presented above as follows:

• **RTO-based RSTEG**: the sender marks a segment selected for hidden communication by distributing the IS across its payload. After successful segment delivery, the receiver does not issue an ACK message. When the RTO timer expires, the sender sends a steganogram inside the retransmitted segment's payload (Fig. 3). The receiver extracts the steganogram and sends the appropriate acknowledgement.

• **FR/R-based RSTEG**: the sender marks the segment selected for hidden communication by distributing the IS across its payload. After successful segment delivery, the receiver starts to issue duplicate ACKs to trigger retransmission. When the ACK counter at the sender side exceeds the specified value, the segment is retransmitted (see Fig. 4). Payload of the retransmit-ted segment contains a steganogram. The receiver extracts the steganogram and sends an appropriate acknowledgement.

• **SACK-based RSTEG**: the scenario is exactly the same as FR/R, but in the case of SACK, it is possible that many segments are retransmitted because of potential non-contiguous data delivery.

6. PadSteg (Padding Steganography)

PadSteg is an inter-protocol steganographic system which utilizes relations between two or more protocols from the TCP/IP stack to enable hidden communication, namely Ethernet with ARP, TCP, UDP and/or ICMP protocols. It is designed for LANs and takes advantage from Ether leak vulnerability, which causes padding in Ethernet frames to be not always set to zeros. To limit the chance of detection PadSteg has so called carrier-protocol hopping mechanism

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

i.e. it switches between different protocols that cause the frame to be padded.
PadSteg operation can be split into two phases:
• Phase I: Advertisement of the hidden node and a carrier-protocol.

• Phase II: Hidden data exchange with optional carrier protocol change.

A steganographic system - *PadSteg* – which is the first information hiding solution based on *inter-protocol steganography*. It may be deployed in LANs and it utilizes two protocols to enable secret data exchange: Ethernet and ARP/TCP. A steganogram is inserted into Ethernet frame padding but one must always "look" at the other layer protocol (ARP or TCP) to determine whether it contains secret data or not. Based on the results of conducted experiment the average steganographic bandwidth of *PadSteg* was roughly estimated to be 32 bit/s. It is a quite significant number considering other known steganographic methods. In order to minimize the potential threat of *inter-protocol steganography* to public security identification of such methods is important. Equally crucial is the development of effective countermeasures. This requires an in-depth understanding of the functionality of network protocols and the ways in which they can be used for steganography. However, considering the complexity of network protocols being currently used, there is not much hope that a universal and effective steganalysis method can be developed. Thus, after each new steganographic method is identified, security systems must be adapted to the new, potential threat.

7. CONCLUSION

Network steganography is currently recognized as a new threat to network security that may be used, among others, to enable data exfiltration or also as the way of performing network attacks. This new type of steganography includes information hiding techniques that utilize, as a carrier, data units and/or their exchange in a telecommunication network. Network steganography can pose a threat to network security, as the current security systems and mechanisms do not provide sufficient countermeasures and are in fact useless against this type of threat. Using steganography for malicious purposes can lead, for example, to confidential information leakage or serve as tools for the distribution of worms and viruses in planning

REFERENCE

[1]M. J. Gross, "Exclusive: Operation Shady RAT - unprecedented cyber-espionage campaign and intellectual-property bonanza," Vanity Fair, August 2011.
[2]S. Adee, "Spy vs. spy," IEEE Spectrum magazine, August 2008, http://spectrum.ieee.org/computing/-software/spy-vs-spy/1.
[3]K. Srivastava, "Congress wants answers on world˝s largest security breach," August 2011, http://-www.mobiledia.com/news/102480.html.
[4]S. Analysis and R. Center, "World˝s largest digital steganography database expands again," SARC Press Release, February 2012, http://www.sarc-wv.com/news/press_releases/2012/safdb_v312.aspx.
[5] R. Anderson, "Stretching the limits of steganography," in Information Hiding. Springer, 1996, pp. 39–48.
[6] Alureon trojan uses steganography to receive commands," September 2011, http://www.virusbtn.com/-news/2011/09_26
[7] Seifert R.: The Switch Book: The Complete Guide to LAN Switching Technology. John Wiley & Sons, 2000
[8] Xylomenos G., Polyzos G.C., Mahonen P. and Saaranen M.: TCP Performance Issues over Wireless Links. IEEE Communications Magazine, April 2001
[9] IEEE 802.11, 1999 Edition (ISO/IEC 8802-11: 1999) IEEE Standards for Information Technology – Telecommunications and Information Exchange between Systems – Local and Metropolitan Area Network – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specif ications

BIOGRAPHIES

Ms. Dhanashri D. Dhobale was born in Sangli, 24th Dec. 1982. She has completed Diploma in Comp. Engg,(ICRE, Gargoti, India, March- 2000) from Mumbai universiry, BE CSE(Walchand college of Engg, Sangli, Maharashtra, India ,March 2005)from Shivaji University and appeared for ME CSE at D. Y. Patil College of Engg, Shivaji university.
She has teaching experience of 8 years and working as an ASSISTANT PROFESSOR in PVPIT, Budhgaon, and Sangli, India. Her 5 papers are selected and registered in different international conferences out of those 2 are explored by IEEE Explorer. She has published 3 paper in international journal.

Vijay Ram Ghorpade, was born in Maharashtra, India, on July 20, 1968. He received the B.E. degree and M.E. degrees in Computer Science and Engineering from Marathwada University, Aurangabad, and Shivaji University, Kolhapur, India, in 1990 and 2001 respectively. In 2008, he earned his PhD degree at SGGSIET, Nanded, India. Presently he is working as Principal at D. Y. Patil College of Engineering and Technology, Kolhapur, India. His research interests include network security and ad hoc networks.