A CHANNEL ANALYSIS IN NETWORK SECURITY – USING A COVERT APPROACH

Raman Kumar[1], Harsh Kumar Verma[2]
[1]Department Computer Science and Engineering, Dr. B.R. Ambedkar National Institute of Technology, Jalandhar, Punjab, India
E-mail : [1]er.ramankumar@aol.in

Abstract

Due to rapid development in the field of communication technologies, security has become the major issue in transformation level data and off-line data. It has further increased the need for online security and authentication for secure information exchange using covert channel and a modified model for data security with data hiding. The objective of this work is to implement a model for network security, using covert channels as a secure environment and covert protocol as a new standard for communication between multi parties but without disclosing the client's details. The most important services to secure communication system are authentication, integrity and confidentiality. In this paper, we also propose a model for construction of secure network computation. Our construction is in the standard model and does not require random oracles. In order to achieve this goal, we introduce a number of new techniques.

Key words : Covert, Channel, Protocols, Language, Uncertainty, Redundancy, Detect ability and Data Hiding.

I. INTRODUCTION

In the era of data transportation through networks the security of data is of prime importance. The network security is the state of chaos due to access of network to every one especially in wireless era. Everyday a new vulnerability is discovered in almost every existing protocol. The answer to these security problems lies in enhancing our proposed solution for data hiding. We will also discuss here about covert channel and old mechanism of data hiding techniques.

II. NETWORK SECURITY AND COVERT CHANNEL

The most important security services to secure communication system are: authentication, integrity and confidentiality, it primarily aims to provide some security means to standard network protocols and security procedures effectively utilizing the available but hidden bandwidth as identified in these standard network processes.

In information theory, a covert channel is a parasitic communications channel that draws bandwidth from another channel in order to transmit information without the authorization or knowledge of the latter channel's designer, owner, or operator.Firstly, Lampson's introduced the notion of a covert channel [1]. Lampson's definition describes a covert channel as one that is used for information transmission, but that is not designed nor intended for communications. The user's system-use expectations will have an impact on the system architecture, size of the kernel and trusted processes, overall system performance, and level of effort required for implementation and formal verification, resource scheduling and management can be performed on a system-global basis. If done on a system global basis, the size of the kernel and trusted processes is increased, the interfaces between the global processes becomes more intricate, verification becomes more difficult and costly, system modification becomes less facile, but system performance improves. If done on local basis with most resource management decisions performed by the system global and perfunctory reconciliations performed by the kernel, the opposite results hold system design, implementation, verification and interfaces are simplified, while system performance may be adversely affected. This basic definition if further analyzed in [3,4] Two parties can communicate in secret if they already share a sufficient quantity of secret information; these analyses elaborate on the concept by associating covert channels with resource allocation policies, shared resources at different system security levels, resource state variable that can be linked with communication taking place within the system [5,6]

A resource state variable, for instance, is any system variable that can be used by a covert channel to signal information from one point to another with in the system. For example, a variable showing files status at several points (states) in the system. In [7], a more complete definition is provided that includes the possibility of covert channels involving access control policy and its implementation. As described in [7], "A covert channel is a communication link between two parties that allows one individual to transfer information to the other in a manner that violates the system's security policy."

Covert channel is classified into covert storage channels and covert timing channels. Communication in a covert storage channel entails the writing of hidden data into a storage location (not meant for communication) by the transmitting party signal information by modulating its own system resources such that the manipulation affects the response time observed by the receiving party.

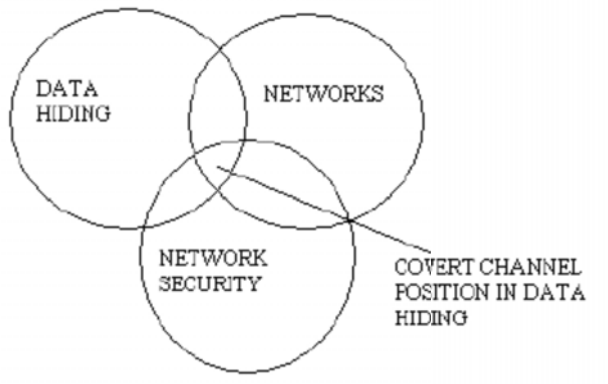

Fig .1 Covert Channel Position Representation in Data Hiding

The covert channel by definition is associated with the violation of system security policy. Such channels therefore pose threat to system security. The other side reflects the availability of unutilized bandwidth on account of the existence of these covert channels.

Aim to investigate covert channels in order to investigate the availability of this unused bandwidth and to associate it with the usage scenario thereby supplementing various network processes and mechanisms.

III. PREVIOUS WORK

A. Data Hiding in OSI Model

In [8], Handel and Sanford take a broader perspective and focus on covert channels within the general design of network communication protocols. They employ the OSI (Open System Interconnection) as a basis for their development in which they characterize system elements having potential to be used for data hiding. The adopted approach has advantages over [9] and [10] because standards opposed to specific network environments or architectures are considered. Foolproof stenographic schemes are not devised. Rather, basic principles for data hiding in each of seven OSI layers are established. Besides suggesting the use of the reserved fields of protocols headers (that are easily detectible) at higher network layers, Handel and Sanford also propose the possibility of timing channels involving CSMA/CD manipulation at the physical layer. The work identifies covert channel figures of merit such as:

- Detect ability: Covert channel must me measurable by the intended recipient only.
- Indistinguishability: Covert channel must lack identification
- Bandwidth: number of data hiding bits per channel use.

More over the properties of system elements which could likely be the containers for data hiding process are mentioned as:

• Uncertainty

• Redundancy

The covert channel analysis presented here, however does not consider issue such as interoperability of these data hiding techniques with other network nodes, covert channel capacity estimation, effect of data hiding on the network in terms of complexity andcompatibility. Moreover, the generality of the techniques cannot be fully justified in practice since the OSI model does not exist per se in functional systems.

B. Data Hiding in LAN Environment by Covert Channels

Girling [9] first analyzes covert channels in a network environment. His work focuses on local area networks (LANs) in which three obvious covert cannels (two storage channel and one timing channel) are identified. This demonstrates the real examples of bandwidth possibilities for simple covert channels in LANs. For a specific LAN environment, the author introduced the notion of a wiretap per who monitors the activities of a specific transmitter on LAN. The covertly communication parties are the transmitter and the wire trapper. The covert information according to Girling can be communicated through any of following obvious ways:

I. By observing the addresses as approached by the transmitter. If total number of addresses, a sender can approach is 16, then there is a possibility of secret communication having 4 bits for the secret message. The author termed this possibility as covert storage channel as it depends in what is sent (i.e.. which address is approached by the sender)

II. In the same way, the other obvious storage covert channel would depend on the size of the frame sent by the sender. For the 256 possible sizes, the amount of covert information deciphered from one size of the frame would be of 8 bits. Again this scenario was termed as the covert storage channel.

III. The third scenario presented is pertaining to the existence sends can be observed by the wire

trappers to decipher for instance "0" for the odd time difference and "1" for the even time difference.

The scenario transmits covert information through "a when-is–sent" strategy therefore termed as timing covert channel. The time to transmit a block of data is calculated as function of software processing time, network speed, network block sizes and protocol overhead. Assuming block of various sizes are transmitted on the LAN, software overhead is computed on average and novel time evaluation is used to estimate the bandwidth (capacity) of covert channels are also presented. The work paves the way for future research. In particular, [9] does not take into account the effect of the existence of covert channel on the overall network performance.

In LAN Protocols point of view covert channel in [10], Wolf presents results that can be regarded as a logical extension of [9], but applied to LAN protocols. Wolf establishes the facts encryption, the basic mechanism of LAN Security cannot ensure the proper blocking of unauthorized information via covert channels. The work points to unused bandwidth possible for covert transmission in mostly used LAN architectures such as IEEE 802.2, 802.3, 802.5 AND 802.7. The focus is on LAN implementations opposed to the architecture itself. The work implies that covert can be expected in every system in which resources are shared. It also highlights the relationship between covert storage channels and protocol format, and the link between covert timing channels and protocol procedures taking into account the frame layouts of the LAN protocols. Covert storage channels utilize the reserved fields, pad fields and undefined fields of the frames.

The fields identified, as means to covertly send information, can easily be detected through the implementation of automated mechanisms. Such mechanisms only monitor such fields, which would discard such frames utilizing these fields irrespective of their purpose.

C. Data Hiding in TCP/IP Protocol suit by Covert channels

A more specific approach is adopted by Rowland [11]. Focusing on the IP and TCP headers of TCP/IP Protocol suite, Rowland devises proper encoding and decoding techniques by utilizing the IP identification field, the TCP initial sequence number and acknowledge sequence number fields. These techniques are implemented in a simple utility written for Linux system running version 2.0 kernels. Rowland simply provides a proof of concept of existence as well as exploitation of covert channels in TCP/IP protocol suite. This work can, thus, be regarded as a practical breakthrough in this research area. The adopted encoding and decoding techniques are more pragmatic as compared to previously proposed work. These techniques are analyzed considering security mechanisms like firewall network address translation.

However, the non-detect ability of these covert communication techniques is questionable. For instance, a case where sequence number field of TCP header is manipulated, the encoding scheme is adopted such that every time the same alphabet is covertly communicated, it is encoded with the same sequence number. Moreover, the usages of sequence number field as well as the acknowledgement field can no made specific to the ASCII coding of English language alphabet as proposed, since both fields take in to account the receipt of data bytes pertaining to specific network packet(s).

The research publications discussed above:

- Identify the existence of covert channels in a network environment.
- Point to devising satisfying techniques of embedding and extraction processes at the source and destination, respectively.
- Do not consider the effect of employing covert communications network as a whole.

These publications, though related with networks, address the data hiding processes as isolated cases. These research contributions therefore, do not explore the existence of covert channels by considering their effect o the overall network environment.

IV. PROPOSED MODEL SOLUTION

According the previous review, have analyzed following field option suitable for covertness. 8 bit hop limit field, initialized to zero for transmission; ignored on reception.

Extension headers:

- Hop-By-Hop Options
- Destination Option Routing
- Fragmentation
- Authentication Header
- Encapsulating Security Payload
- Destination Options (for options processed only by the final destination)

A technique look IPv6 secure covert channels And data hiding algorithm that can pass supplementary

information through most firewalls and intrusion detection systems.

In information theory, a covert channel is a parasitic communications channel that draws bandwidth from another channel in order to transmit information without the authorization or knowledge of the latter channel's designer, owner, or operator, covert channel is so called because it is hidden within the medium of a legitimate communications channel. Covert channels typically manipulate certain properties of the communications medium in an unexpected, unconventional, or unforeseen way in order to transmit information through the medium without detection by anyone other than the entities operating the covert channel.

All covert channels draw their bandwidth (information-carrying capacity) from a legitimate channel, thus reducing the capacity of the latter; however, the bandwidth drawn from the channel is often unused, anyway, and so the covert channel may still be well hidden. For example, steganography is a form of covert channel in which very small details of images (or other multimedia files) are subtly altered in order to communicate information in a way not immediately obvious to anyone casually examining the images.

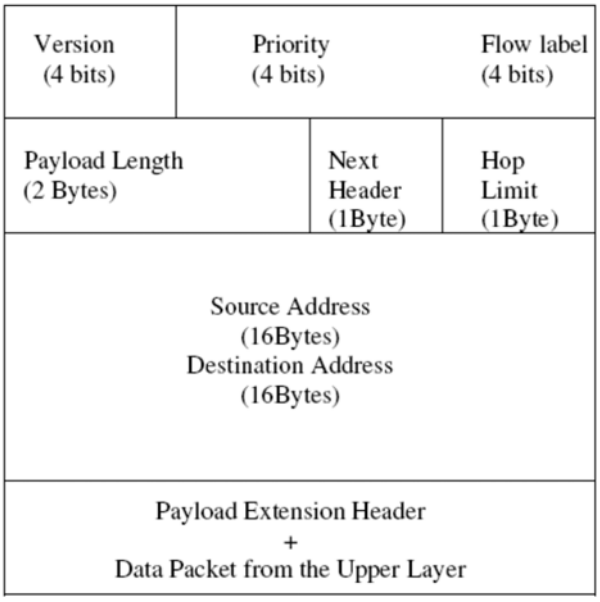

Fig. 2 Block diagram of field options for Covertness

One type of steganography uses the low-order bit of the data for each pixel in an image to carry the information of a covert channel: these bits carry the covert message, while the rest of the bits carry the legitimate image. The very slight change in the image caused by modification of the low-order bit in each pixel is imperceptible in most cases to anyone who is not already looking for such a change. The field options for covertness as shown in Fig. 2.

Proposed model solution for secure communication is given below:

The proposed solution consists of Data to be hidden Dk and Network Packet Pk and again applied for the Stegno algorithm in addition to this secret key is also added. Then they are passed through channel with the help of packet and Extraction or Detection process to obtain the Intended data.

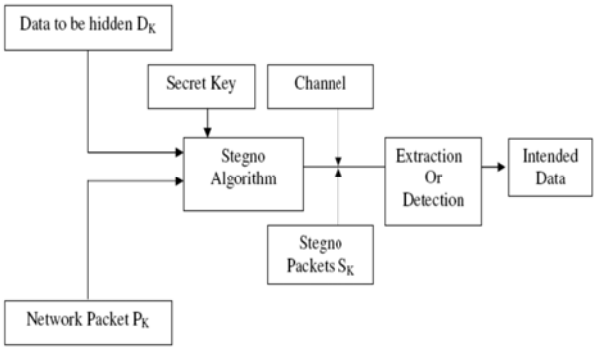

Fig. 3 Block Diagram proposed for the secure communication

V. CONCLUSION

As the communication technologies gains popularity, it is important to understand the characteristics of these channels and protocols so they are turned to achieve security. In sum, network security is always a big issue. Network attacks just reflect various problems in the existing network architecture and protocol organization. In physical world, terrain and atmospheric conditions exists which affect network connectivity. We just categorize them and list some possible ways to deal with them. It has been shown that as the how security can be achieved using a covert channels approach.

ACKNOWLEDGEMENT

I am deeply indebted to my supervisor Dr Harsh Kumar Verma from the Department of Computer Science and Engineering, Dr B R Ambedkar National Institute of Technology, Jalandhar, Punjab, India whose help, stimulating suggestions and encouragement helped me in all the time of research for and writing of this paper for journal.

REFERENCES

[1] Lampson B. W., October 1973, “A note on the confinement problem”, in Proceeding of the Communication of the ACM, no. 16:10, pp 613-615.

[2] Lipner S. B., November 1975, “A comment on the confinement problem”, operating system review, vol. 9, pp 192-196,.

[3] Schaefer M., Gold B., Linde R., and Schieid J. October 1977, "Program confinement in kvm/370", Annual ACM Conference,

[4] Huskamp J. C., 1978 , "Covert Communication Channels in Timesharing Systems", Technical report UCB-CS-78-02,Ph. D Thesis, university of California, Berkeley, California.

[5] Denning D. E., 1983, "Cryptography and Data Security, Reading", Massachusetts: Addision-Wesley, reprinted ed.

[6] Kemmerer R. A., August 1983, "Shared resource matrix methodology: An approach to identifying storage and timing channels", ACM Transactions on computer systems, vol 1 to 3, pp-256-277.

[7] Supersedes CSC-STD-001-83, Department of defense, December 1985 "Department of Defense trusted computer system evaluation criteria", Tech Rep. DOD 5200.28-ST.

[8] Handel T. and Sanford M., May-June 1996,"Hidding data in the OSI model network model", First International Workshop on Information hiding, Cambridge, U.K.

[9] Griling C. G. February 1987, "Covert channels in LANs", IEEE Transactions on Software Engineering, vol. SE-13 of 2,. 292-296

[10] Wolf M., 1989, "Covert channels in LAN Protocols", In proceeding of workshop on Local Area network security (LANSEC' 89) (T.A. Bersonand T. Beth, eds,) pp. 91-102.

[11] Rowland C. H., July 1997, "Covert channels in the TCP/IP Protocol suite", Tech Reep. 5, First Monday, Peer Reviewed Journal on the Internet.

[12] Katezenbeisser S. and Petitcolas F., 2000 "Information Hiding Techniques for Stegnanography and Digital Watermarking", Computer Security Series, MA 02062; Artech House, Inc.

Mr. Raman Kumar, is presently a Research Scholar in the Department of Computer Science and Engineering. Dr. B.R. Ambedkar National Institute of Technology, Jalandhar, Punjab. His area of research is Information Security.