Ephemeral Feature Presentation of Covert Channels in Network Protocols

Prof. RajeswariGoudar*, SujataEdekar**

Computer Department, Pune University
MAE Alandi, University of Pune 411015,
Maharashtra India
rmgoudar66@gmail.com

***Abstract*-** Covert channels leaks information where information travels overlooked. Encryption used to protect the communication from being deciphered by unlawful users. But covert channels hide the presence of communication. Covert channels are serious security intimidation. There are many existing techniques available for development of covert channels by influencing certain fields in the network protocols such as HTTP, IP, TCP, etc. The available packet length based covert channels are having tamper resistance capability but due to abnormal traffic distribution results in recognition possibility. In this paper we present overview of different protocol as well as some packet length based covert channels.

***Index Terms*-** covert channels, packet length, high bandwidth, network protocols,packet payload,computer network

I. INTRODUCTION

Computer networks are a vital part of our lives. The different fields like educational system, commerce, banking organizations, industry, military everywhere we witness the manifestation of computer networks. Computer networks is linking tool for communication and association of information. Due to exposed information security facets of information is indispensable. Information Security has now become everyone's prerequisite, either directly or indirectly associated with network environs. The information may include the share market values, the database of the company, the quotations; military secrete data, and so on. So basically the information can be video, audio or in text form. The transfer of information is done by gmail, rediffmail such applications for mailing and for video conferencing Skype like applications are used. But due to this the need of information or the data security also increased in proportion to the data.

There are many techniques that are present in the market and explained in the academia also for the secure communication. Different cryptographic algorithms, data hiding techniques are used for information security. Encryption can just oppose the unauthorized access by third party, compared to these covert channels data hiding techniques are used for hiding the presence of the communication [6].

The covert channels are a great threat to information security as the communication is carried out undetected. The performance of the system and the network get affected due to the hidden and unclear (may be illegal) use of resources or functions of the covert channel.

II. RELATED WORK AVAILABLE TECHNIQUES

Covert channels are used for confidential data communication during transmission. Lampson focused on covert channels and represented the concept firstly in 1973[1].According to him covert channels are divided into storage, legitimate and covert categories. Covert channels are also classified as storage and timing channels [13, 22].

In paper [16] presented some characteristics of Covert Channels like behavior, path, spread, efficiency. Various other parameters to be considered to characterize covert channels were introduced in [20] as noise, bandwidth, synchronization and aggregation.

Classification of Covert Channels:

There are mainly two types of covert channels, which are storage and timing channels.

Storage Channels:

- It implicates process writes at the storage place and another process reads it directly or rather indirectly.
- Examples of storage locations are disk space, print spacing, and file naming.

Figure 1: Example Storage Channels

Timing Channels:

- In timing channels, Hints information to another by using modulation effect of system supply (resource) such that the manipulation of the response time by second process gives the hidden information.
- The events that can be utilized as timing channels are CPU utilization, Resource availability etc.

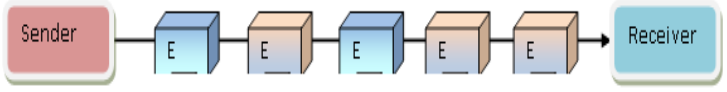

Figure 2: Example Timing Channels

Applications of Covert Channels:

Covert channels are exclusively used for message communication over space as a reliable signal carrier. Therefore it is having few permissible and many unlawful applications [6] as:

1. Communication by security organizations so as to cover their passages and practices.
2. Snooping
3. Information trafficking
4. Paul Henry [4] mentioned that, numerous malicious programs make use of covert channels for setting DDos attack.
5. Conveying encoded data covertly in which application harmless and untraceable transmission is vital.
6. Hacking of the information
7. In the organization or system information leakage.
8. Information hiding to repudiate its presence.

III. AVAILABLE TECHNIQUES

There are many techniques based on covert channels. But there are many factors like delay measurement, network conditions, congestion, traffic load etc. Due to which timing channels are may get affected by noise. So we are basically considering storage channels. There are many techniques available which utilizes packet header unused or reserved bits as covert channels.Ahasan[5] introduced IP's Don't fragment bit as covert channel whereas Sebastian Zander[11] used IP protocol's TTL field .TTL fields in IPv6 are referenced in [15,18,19]

LAN Environment Covert Channels

Girling [3] first consider network covert channels. He concentrated on local area networks (LANs) and identified three obvious covert channels (one timing & two storage channels). This demonstrates the real examples of the bandwidth possibilities for simple covert channels in LANs. For a definite LAN setting, the author hosted the view of a wire tapper which observes events of a particular transmitter on LAN. The covert communication is carried out in between the wire tapper and transmitter. To calculate the transmission time for a data block calculated following factors are considered: time for software processing, speed of the network, protocol overhead and block size of network. By assuming transmission of different size of blocks on the LAN, based on novel and average time evaluation the software overhead is figured out to evaluate the covert channel capacity (bandwidth). Besides, way out for decreasing the covert channel bandwidth is also offered. Besides, way out for decreasing the covert channel bandwidth is also offered. To be precise, [3] does not considered the effect of the presence of covert channels on performance of overall network conditions.

LAN Protocol Covert Channels:

In [24], the results offered by Wolf can be observed as a logical extension of [3], but used with LAN protocols. Wolf institutes the point that encryption, which is used for LAN security, cannot safeguard the suitable blocking of unlawful info through the covert channels. The work focus on the idle bandwidth promising for covert communication in the most frequently used LAN architecture standards like IEEE 802.2, 802.3, 802.4, and 802.5. The motivation is on LAN implementations contrasting to the architecture itself. The thesis denotes that in each system where shared resources are used the existence of covert channels can be expected. Author highlights the association between protocol format and covert storage channels as well as the relationship between protocol technique elements and covert timing channels by considering frame layouts of the LAN protocols. Padding field, the reserved fields and unused fields of the frame are used by the Covert storage channels. By applying programmed mechanism the detection of the fields identified (which is used as means to covertly send information). Such type of mechanisms just monitors such type of fields, which would dispose of such frames using these fields regardless of their purpose.

OSI Model Covert Channels:

In paper [14], Handel and Sanford focussed on focus on network protocol covert channels with wide perspective. They referenced the OSI (Open System Interconnection)model as a base for covert channel to hide the data .The accepted method has advantages over [3]and [24] due to the standards divergent to particular network environments or architectures are considered. Flawless stenographic schemes are not developed. Instead, basic principles for hiding the data in each OSI layers are designed. Moreover proposing the use of the protocol header's reserved fields (are detected easily) at high network layers, authors also recommended the probability of CSMA/CD manipulation at the physical layer as timing channels. The merits of covert channels are figured out in this paper such as

- Detectability: Covert channel must be determinate simply by the envisioned recipient.
- In distinguishability: Covert channel must pretend like overt channel.
- Bandwidth: With respect to covert channel the number of hidden data bits per channel use is bandwidth.
- Uncertainty and Redundancy.

But the downside of in this paper are the issues such as data hiding effects with respect to compatibility and complexity on the network ,interoperability of the covert data practices with other network nodes, bandwidth estimation of covert channel.

TCP/IP Protocol Suite Covert Channels:

Covert channels in the TCP and IP headers of TCP/IP protocol suite are introduced in a specific way by Rowland [10]. Rowland developed suitable encrypting and decrypting techniques by using the fields such as the TCP initial sequence number, IP identification field, and acknowledgement field , sequence number fields. These approaches are designed in a utility service written for Linux systems with version 2.0. Rowland delivered an idea of the presence as well as the manipulation of covert channels in TCP/IP protocol suite. The implemented encrypting and deciphering techniques are more logical in comparison with earlier proposed work. These techniques are evaluated after considering security methods such as network address translation and firewall. Still, the secret communication method's non-detectability is doubtful

Retransmission Covert Channels:

Many other innovative and impressive techniques are also available like RSTEG [8] and CLACK [12]. In [8] authors have presented retransmission mechanism by using covert channel in all type of network protocols as shown in the figure 3. In this design purposely invoked retransmitted packet which are used to carry a covert data in the payload field of the packet.

Retransmission Steganography (RSTEG) doesn't send successive acknowledge for received packet to sender. This is the provision to deliberately appeals retransmission. RSTEG returns acknowledgment to positively received packets as well as for purposefully invoked retransmission packets. The author used TCP retransmission process as covert channel. The RSTEG algorithm can be used along with timeout for Fast Retransmit/Recovery (FR/R) Retransmission (RTO), Selective Acknowledgement (SACK). The difference between normal retransmitted packets with purposefully invoked retransmitted packet is carried out by sender by marking the intended packets for covert information. There is a secret Stego-Key (SK), and a hash function (H) is used to calculate the Identifying Sequence (IS) for covert information which is shared by both the parties sender and receiver. RTO-based retransmissions for avoiding the detection should be utilized in RSTEG.Also the planned retransmissions are produced in a natural way. However, SACK-based RSTEG is efficient for maximizing the stego bandwidth. RSTEG can also be used for IPv6 and IPv4 for covert communication. The author confesses about the scheme that it can be detected, during excessive intentional retransmissions.

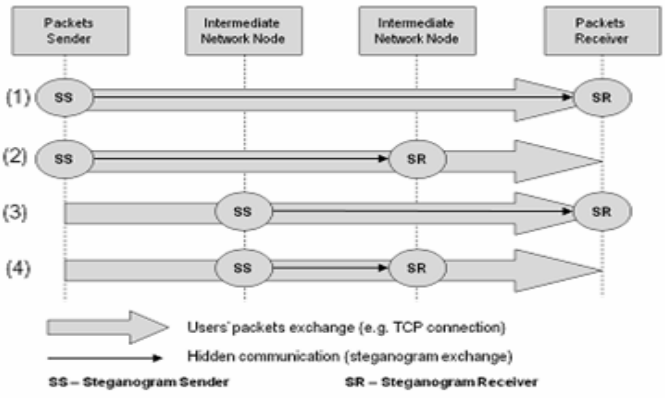

Figure 3: Retransmission Covert Channel

Acknowledgment Field Covert Channels:

Sending data in the ACK field of the packet is another different concept, shown in figure 4 presented in CLACK [12]. In paper [12] authors presented CLACK .This method uses partial acknowledgments. The encoder in CLACK inserts covert data in partial acknowledgments (ACKs) field of a TCP and manages the TCP data led from the server as acknowledgments for transmitting hidden information. Besides other techniques in CLACK the TCP receiver is an encoder and a decoder is actually a sender. The covert message is engraved in the ACK field of TCP by the encoder. CLACK encoder only desires to receive the data and forward the pure ACKs.There are certain constraints of the scheme like there should not be any retransmission, ideal network condition i.e. Should be lossless, and packet ordering must be preserved. In this technique the server has to continuously send the data and Nagle algorithm should be off.

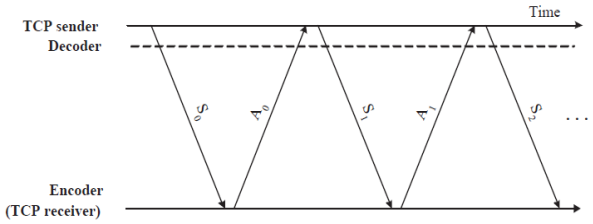

Figure 4: CLACK: Sending of data &Ack

Packet Length Based Covert Channels:

There are specific models which uses the packet length for designing the covert channels. Link layer frame length utilization for hidden communication is proposed by Padlipsky [7] and Girling [3].In this [3, 7] link layer frame length is mapped to each byte of covert message. So ultimately at least 256 message lengths are needed for single hidden byte. Predefined message lengths are used by sender and receiver. The main disadvantage of this system is the communication is detectable due to the statistical computations. The reason is due to predefined length (not real time) abnormal (not real) network traffic distribution.

LAWB model was proposed by Yao [21] in 2008.But due to abnormal traffic it's vulnerable to detection. Like our proposed model sender and receiver has shared a secrete matrix. The matrix is filled with unique packet length L .For sending a message sender selects a row ID as a covert message, and from the matrix selects a random cell in that row denoted by Len. When the packet arrives at receiver end it checks for the rowid of the cell in which the L contains. Periodic matrix transformation at both the sides is implemented by the author [21].

One more packet length based algorithm is introduced by Liping and Ji [9] in which the model is based on normal traffic distribution. As a Reference normal packet lengths from the network are captured from both ends of the system. The packet length to be transmitted is randomly selected from the list of Reference as well as the length for the next packet is generated by adding the covert message and send to the receiver. The reference list is modified by the sender when the packet sending is over. After arrival of the packet at receiver end, it extracts the covert data from the packet length received with the help of Reference list. The major drawback of this system is the newly generated packet length sometimes doesn't fit in normal length traffic distribution which results in detection of covert communication.

In the next paper of LipingJi [17], he introduced Normal Traffic Network Covert channel. In this the real time packet lengths are taken as a Reference in sorted order. Equal size of buckets with specific packet length range is arranged. While sending the data sender select the group of covert bits and convert them into equivalent decimal. By selecting the equivalent decimal bucket with reference to packet length list, sender randomly selects the packet length from the bucket and sends it to receiver. At receiver end, checks for packet length and search into reference bucket range. If the bucket found the bucket number is nothing but the required covert data. This technique is utilizing normal packet lengths. The sender maintains the reference list at his end and receiver maintains the bucket ranges so the advantage of the technique is time and space efficiency. But if seen statistically

then a pattern can be formed and detection is possible due to constant transmission which never gets updated. Also the covert data carrying capacity is low as compared to our technique.

In the paper [2] author Hussain approached packet length based covert channels. It can be said that it's the advance version of previous algorithm [17].He presented an idea of tamper resistant model. In this he utilized the stego column concept which is the heart of the system. In this the matrix of real packet length is shared rather pre shared by both parties. The message need to be converted into its binary form and chunks of w bits (2, 3, or 4) grouped together to select a row in the matrix. According to any random cell selection in that row decides how to send the data. If the cell fall in the stego column then data is transferred as the payload else the rowid itself is the covert data.

In the paper the above paper is further enhanced by two features capacity improvement and added security feature in paper[23].In this paper along with the stego column the stego row concept is used in which the stego row will append the data at receiver side to the selected rowid to form the message. For security improvement the encoding of the payload is introduced in this paper. It utilizes normal network communication messages for referencing the length of the packet. The main advantage of using the real time packet length is for achieving undetected data transmission due to normal traffic distribution. Packet length based methods are important with respect to the quality of attack resistant.

IV. CONCLUSION

Now from the different algorithms we can conclude that there are many techniques available as covert channels. There are many base papers from which we can improve the existing covert channels as well as can research on detecting the covert channel mechanisms so that they can't be used for unlawful purposes. As a future work the combination of different network protocols can also be used as hybrid model. In this case again in a random fashion we can utilize the protocols and rearrange the message at the receiver side.

REFERENCES

[1] B. Lampson. A note on the confinement problem.Communications of the ACM, 16(10) : 613 - 615, October 1973.

[2] Mehdi Hussain,M.Hussain ,"High Bandwidth covert Channesl in network protocol",IEEE Computer ,2011

[3] C. G. Girling, "Covert channels in LAN's", IEEE Trans.Software Engineering , vol. SE-13, no. 2, pp. 292âAS96, Feb. 1987.

[4] Paul Henry,"Covert channels provided hackers",CyberGuard Corporation.

[5] K. Ahsan, D. Kundur, "Practical data hiding in TCP/IP",ACM Workshop on Multimedia Security, December 2002.

[6] Kashif Ali Siddiqui,"Covert channels in TCP/IP and Protocol Steganography" ,A Survey report,2003.
Covert Channels Using Chi-Square Test",IEEE ,2009

[7] M. A. Padlipsky, D. W. Snow, and P. A. Karger,"Limitations of end to -end encryption in secure computer networks", Tech. Rep. ESD-TR-78-158, MitreCorporation, August 1978

[8] Mazurczyk W., Smolarczyk S., Szczypiorski K.,"Hiding Information in Retransmissions",In Computing Research Repository (CoRR),abs/0905.0363, arXiv.org E-print Archive, Cornell University, Ithaca,NY (USA), May 2009.

[9] Liping Ji, Wenhao Jiang, and Benyang Dai,"A novel covert channel based on length of messages", International Conference on e-Business and Information System Security, 2009.

[10] C. H. Rowland, "Covert channels in the TCP/IP protocol suite," Tech. Rep. 5, FirstMonday, Peer Reviewed Journal on the Internet, July 1997.

[11] Sebastian Zander, Gernville Armitage, and Philip Branch,"A Survey of Covert Channel and Countermeasures in Computer Network Protocols", IEEE Communications Surveys and Tutorials, vol 9, no.3, pp. 44-57, 3rd Quarter 2007.

[12] Xiapu Luo Chan, E.W.W. Chang, R.K.C"CLACK:A Network Covert Channel Based on Partial Acknowledgment Encoding". ICC'09. IEEE International Conference on 14-18 June 2009.

[13] Pukhraj, Singh. Whispers on the Wire, Network Based Covert Channels,White paper,gray-world.net/papers/pukhrajsingh covert.doc

[14] T. Handel and M.Sandford., "Hiding data in the OSI network model," (Cambridge,U.K.), First International Workshop on Information Hiding, May-June 1996.

[15] Zander, Sebastian. Grenville, Armitage, Philip Branch." Covert Channels in the IP Time To Live field", Center for Advanced Internet Architectures (CAIA), Swinburne University of Technology, Melbourne,Australia

[16] Marc Smeets, Matthijs Koot. Research Report: Covert Channels. University of Amsterdam, MSc in System and Network Engineering, 2006

[17] Liping Ji, Haijin Liang, Yitao Song, Xizmu Niu,"A Normal Traffic Network Covert Channe", Computational Intelligence and Security,2009.

[18] T. Handel and M. Sandford, "Hiding Data in the OSI Network Model" ,Proc. 1st IntâAZl. Wksp. Information Hiding, 1996 pp. 23 âAS 38.

[19] C. Abad,"IP Checksum Covert Channels and Selected Hash Collision",tech. rep., UCLA, 2001.

[20] A guide to understanding Covert Channel Analysis of Trusted Systems , National Computer Security Center, Maryland, USA. 1993.

[21] YAO Quan-zhu and ZHANG Peng, "Coverting channel based on packet length", vol.34 No.3 Computer Engineering, February 2008.

[22] U.S. Department of Defense. Trusted Computer System Evaluation "The Orange Book " Publication DoD 5200.28-STD. Washington : GPO 1985 , http :// www.radium.ncsc.mi l/ tpep/ library/ rainbow/ 5200.28-STD.html

[23] Sujata Edekar,Rajeswari Goudar,"Real time length utilization for covert communication in network protocol",International conference on electrical engineering & computer science,ISBN978-93-83060-02-3,2013

[24] M.Wolf, "Covert channels in LAN protocols," in Proceedings of the Workshop onLocal Area NetworK Security (LANSEC'89) (T.A.Berson and T.Beth, eds.), pp. 91– 102, 1989.

AUTHORS

First Author –
Prof.RajeshwariGoudar
M.E. Computerengineering
Professor in Computer Department, MAE Alandi, University of Pune 411015,
rmgoudar66@gmail.com

Second Author –
SujataEdekar
B.E. Computer Technology, pursuing M.E. Computer Engineering from MAE Alandi, University of Pune 411015,Working as professor in BSIOTR(W),Pune University
sujata.edekar@gmail.com