Covert Channels:" Emerged in mystery and departed in confusion"

Rajeswari Goudar[†] and Sujata Edekar[††],

Computer Department,
MAE Alandi, University of Pune 411015, Maharashtra, India

Summary
Due to rapid change and development of network technology in the current changing business environment, there is an increased communication and exchange of information being carried over the internet, where we demand them for official and personal needs to communicate with customers or with employees of organizations, for money transactions, to retrieve information or shopping etc. The usages are endless and the security of our systems has to be increased and the security of our networks has slightly been enhanced, still lots of security problems exist, especially in enterprise and private networks. The encryption protects the information from unauthorized viewer, but the covert channel hides the existence of the communication where they are used for secret transfer of information on network. This can be a good thing if covert channels are used to protect privacy or increase security of precise data communication. Covert channels do not exist in practice and are not the part of any network protocol, where they take advantage of existing protocols to transfer the information like TCP/IP.

Key words:
Covert Channel, network security, steganography, encryption.

1. Introduction

Nowadays digital communication has become an essential part of infrastructure and lots of applications are internet based. In many cases it's desired that communication is to be made secrete, for exchanging of confidential data like credit card numbers, passwords etc. As the number of users increase, there is need for protecting information in terms of transmission and storage. Hence the information security can be achieved by using steganography ,cryptography ,network covert channels or combination of them can be used .Steganography is a process of hiding the information or messages in appropriate carrier file whereas cryptography is nothing but possibly decoding the information.

Using the hidden channels of communication during a time of war was not a new idea. This method had been used thousands of years ago when messages were communicated via wax tablets that were inscribed with a wooden stylus [8]. Present-day covert channels utilize modern technology and the network provides a medium for transport of information. Covert channels for information hiding were introduced in 1973 by Lampson [1] to avoid information leakage where a covert channel is widely applied in computer networks to hide the existence of communication and to secure data transmission. Covert channels exist in most communications systems which allow individuals to communicate undetectably. However due to their complexity covert channels are rarely used.

Encryption is used in communication for protection from being decoded by unauthorized parties, but covert channels are used to hide the existence of the communication. Covert channels are used for the secret transfer of information. A channel can be defined as a communication path by which information can flow within a computer system. A channel is called as overt channel which is designed for the authorized transfer of data whereas covert channel is a path that can allow information to flow in a manner that violates the security policy of a system, allowing the transfer of information by an unauthorized process [15].

Covert channels often are used to describe the idea of hiding any type of information in any type of medium and steganography can be included in covert channel communication as stenography is used for hiding of data inside binary files, audio files like .wav, .mp3, .au or digital images like .jpg, .gif, and .bmp and other binary formats such as executable. So stenography can be included in covert channel communication.

A covert channel is designed to be hidden within the normal communication traffic of a legitimate logical channel, such as TCP or UDP. Synchronization variables or information used by a sender and a receiver for covert channels may be used for operations on multiple data variables. We say the channels are aggregated, depending on how the sender and receiver set, read, and reset the data variables, channels can be aggregated serially, in parallel, or in combinations of serial and parallel aggregation to yield optimal bandwidth. Otherwise the channels are non-aggregated [5]. If all data variables are set, reset and read serially then the channel is serially aggregated. Parallel

Manuscript received November 5, 2011
Manuscript revised November 20, 2011

aggregation of covert channel variables requires, for bandwidth maximization reasons, that the sender and receiver pairs be scheduled on different processors at the same time as a group.

Section 2 explores details of covert channel followed by characteristics of covert channel in section 3.Classification of covert channels and some of covert channels used in network protocols are explained in section 4.

2. Covert Channels

Covert channels are effective means of information hiding and secret communication in public computer networks. The term covert channel describes a secret communication technique employed by two or more parties allowed to exchange information, while they assume the data channel in use is under surveillance. Thus, they modify the content of the genuine low security message or the envelope used to carry this message, so that eavesdropper cannot read from the secret channel. In covert channel scenarios, A is often considered to be an inmate of a high security prison. It is assumed that he knows an escape plan from a prison where B is spending his sentence. A is trying to send the escape plan to B, however W ,the warden checks their communication very precisely, thus they employ covert channel known to them to send the secret messages as shown in fig 1.

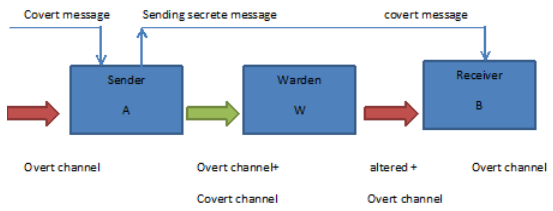

Fig. 1 Communication Model

An information flow policy is typically designed to preserve the confidentiality and/or integrity of data within a computer system. In terms of confidentiality the policy tries to prevent the flow of information to those users not authorized to receive it. In Multi-level Security (MLS) systems it's important to allow information flows between users of the system who have sufficient security clearances; and to prevent flows to those that do not. If all possible information flows can be identified then these flows can be restricted such that the goals of the security policy are preserved. If it is not possible to identify all such flows then there is the potential for information to flow in an unauthorized manner. If information can flow within a system in an unauthorized manner then the security boundaries defined by the security policy can be violated. It is possible, even in systems that have security policies as well as discretionary(DAC) and mandatory access controls(MAC),]that information may be able to flow in a manner not expected by the designers of the system[9]. It has been shown that a limitation of the Bell-LaPadula Model [10] is that it cannot constrain information flow in such a way to prevent the establishment of channels.

3. Covert Channels Characteristics

Covert Channels are hidden and they have the same characteristics than other communication channels [6]. The covert channels can be active which generates its own traffic whereas passive covert channel piggybacks on traffic generated by other processes. Some of the characteristics of covert channel are capacity, transmission mode, noise, path to be followed between sender and receiver which are explained as below.

Capacity: It is the quantity of information that can be transmitted through the channel. Capacity is a very important part of the global quality of a channel. From a security point of view, a larger capacity channel will make possible for more information to leak. On the other hand capacity may impact the overall furtively of the channel when this one relies on usual but quiet channels.

Noise: It is the amount of perturbations that can interfere with the information while it is transmitted through the channel; Noise will highly rely on the nature of the channel. Storage channels are usually not very sensitive to noise as probabilities for a process not to be able to write on a file it owns are quite low. On the opposite timing channels are very noisy because of the number of external factors that can have an impact on execution time of a process.

Transmission Mode: It can be synchronous when the information is received and managed on the fly by the destination entity otherwise asynchronous. In any scenario of covert channel exploitation, one must define the synchronization relationship between the sender and the receiver of information. Thus, covert channels can also be characterized by the synchronization relationship between the sender and the receiver. The purpose of synchronization is for one process to notify the other process it has completed reading or writing a data variable. Therefore, a covert channel may include not only a covert data variable but also two synchronization variables, one for sender- receiver synchronization and the other for the receiver-sender synchronization. Any form of

synchronous communication requires both the sender-receiver and receiver-sender synchronization either implicitly or explicitly [11]. Note that synchronization operations transfer information in both directions, namely from sender to receiver and vice versa and, therefore, these operations may be indistinguishable from data transfers.

Spread: The sender splits data to multiple (logical) intermediate hops, after which the data is converged to the receiver. Alternatively, the sender can send the data to a single host with multiple IP addresses. This path is the stealthiest of all.

4. Covert Channels Classification

Some define covert channel as a communication channel for information transfer, some as security violation. Later covert channels are presented based on their common usage, such as resource allocation policies, shared resources at different system security levels, resource state variables and resource management implementations. A communication channel is covert if it is neither designed nor intended to transfer information at all [1].A communication channel is covert (e.g., indirect) if it is based on "transmission by storage into variables that describe resource states "[3]. It is a communication channel that can be exploited to transfer information in a manner that violates the system's security policy [4].

Covert channels can be classified by different aspects. Girling pointed out three kinds of covert channels with respect to network in general as time, length and address [7]. Even though the classification is of different types we can aggregate all the types under storage & timing channels as shown in fig. 2. The protocol based or non-aggregated can be merged into storage, and frequency based can be merged into timing channels.

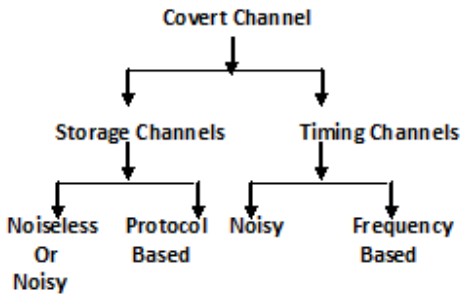

Fig. 2 Classification of Covert channels

Storage Channel: is one which involves the direct or indirect writing of a storage location by one process and the direct or indirect reading of the storage location by another process [4].

Timing Channel: is one which involves a process that signals information to another by modulating its own use of system resources e.g., CPU time in such a way that this manipulation affects the real response time observed by the second process [4].

Protocol Based covert channel: It exploits ambiguous or non- uniform features in common protocol specification [13].Network protocols such as HTTP, DNS, TCP, IP are some examples of protocol based covert channels [14].

Frequency Based covert channel: In this information is encoded over many channels of covert traffic. The order or combination of covert channels access encoded information [13].

Noiseless channels: As with any communication channel, covert channels can be noisy or noiseless. A channel is said to be noiseless if the symbols transmitted by the sender are the same as those received by the receiver with probability 1. That is, regardless of the behavior of other user processes in the system, the receiver is guaranteed to receive each bit transmitted by the sender. In direct client-server HTTP connection, covert channels is characterized as Noiseless since hidden payload is stored within an object originating from a sender and transmitted directly to the receiver. Matt defines [12] the noiseless channel as a covert channel that uses a resource available to the sender & receiver only.

Noisy Channels: Whenever extraneous processes-not just the sender and receiver-use the shared resource, the bits transmitted by the sender may not be received correctly with probability 1 unless appropriate error-correcting codes are used. The error-correcting codes used depend on the frequency of errors produced by the noise introduced by extraneous processes and decrease the maximum channel bandwidth. The protocol based DNS can be noisy as the DNS cache can be accessed and modified by any system connected to internet. According to Matt, [12] the noisy channel is that which uses the resource available to subject other than the sender and the receiver.

Which covert channels are of concern is dependent on what attackers can observe of the computing system. For example, power channels are important for smart cards, because they must draw their power from the untruth terminal into which they are inserted. A program that is secure on an abstract computer with no power requirements might be part of a larger, insecure system when it is run on a real computer. Thus a computing

system can be said to protect confidential information only with respect to a model of what attackers and users are able to observe of its execution. These channels are dangerous when the attacker can repeatedly run a computation and observe its stochastic properties.

Covert channels used in network protocols

Some of covert channels used in TCP/IP are the IP packet identification field, TCP initial sequence number field, TCP acknowledged sequence number field. There are many fields that are not used for normal transmission or are "optional", to be set as needed by the sender. It is also possible to send secret information in the MAC 802.11 header. It is a covert channel implemented in the sequence control and the initial vector fields armed with some security measurements to avoid to be detected by network sniffers. It is used for hidden file transfer using file transfer protocol and to send hidden short messages.

5. Conclusion

Covert channels allow us to more adequately include a broader base of information-hiding mechanisms than normally associated with steganography. Even though it may take considerable processing to send one bit of data through the channel; error control coding is needed to signal reliably through a noisy covert channel. We have given an overview of covert channels which are useful for secret communication and described the existing covert channel characteristics. There are many possibilities of creating covert channels in computer network protocols .A comprehensive classification of the different covert channels is elaborated in brief. However development of new covert channels with improved stealth and capacity and developing more effective detection and elimination techniques will carry on. Covert channels are useful in IP header tunneling, DNS tunneling, HTTP entity tag tunneling, covert encoding or steganography and many more. Many applications of covert channel are of malicious or unwanted nature, so it's a serious threat to network security. Covert channels can send messages outside the logical construct of everyday computer applications. Data can be hidden anywhere and in many different ways.

References

[1] B. Lampson, "A Note on the Confinement Problem", Communication. ACM, vol.16, no.10, Oct 1973, pp. 613-615.

[2] Dario Forte, Covert Channels: Covering 'Malicious', Network Security, Volume 2003, Number 4, April 2003 , pp. 16-18(3).

[3] M. Schaefer, B. Gold, R. Linde, and J. Scheid, "Program Confinement in KVM/370," Proceedings of the 1977 Annual ACM Conference, Seattle, Washington, ACM, New York, pp. 404-410, October 1977.

[4] NCSC (National Computer Security Center),Department of Deference Trusted National Computer Security center ,1985

[5] V. D. Gligor and C. S. Chandersekaran, "Towards the Development of Secure Distributed Systems," in Grissonnanche, A. (editor), Information Security: The Challenge, IFIP Press, Monte Carlo, pp. 395-406,1986.

[6] Renaud Bidou Radware, Frédéric Raynal, Covert Channels, MISC Magazine, 2011.

[7] C.G. Girling, Covert Channels in LAN, IEEE Vol SE-13, No.2, 1987, pp. 292-296.

[8] Russ Rogers, Matthew G."Hacking a Terror Network: The Silent Threat of *Covert Channels*", Network Protocols,2005

[9] Trusted Computer System Evaluation Criteria, United States Department of Defense. December 1985. DoD Standard 5200.28-STD.

[10] Hansche, Susan; John Berti, Chris Hare (2003). *Official (ISC) 2 Guide to the CISSP Exam*. CRC Press. pp. 104.

[11] http://www.iv2-technologies.com/CovertChannels.pdf.

[12] Matt Bishop, Reference book "Computer Security: Art and science", Addison –Wesley Professional, 2003.

[13] S.J. Murdoch, S. Lewis," Embedding Covert Channels into TCP/IP", University of Cambridge, United Kingdom 7th *Information Hiding Workshop, June 2003.*

[14] Marc Smeet, Matthijs Koot, Research Report: Covert Channels, RP1University of Amsterdam, MSc in System and Network Engineering, 2006.

[15] Tsai, C. R., Gligor, V. D., & Chandersekaen, C. S. June , Formal Method for the Identification of Covert Storage Channels in Source Code, *IEEE Transactions on Software Engineering*, **16**/6, 569- 580,1990.

Author

Rajeshwari Goudar received Bachelor Degree from Karnataka University & post graduate degree in Computer engineering from Kolhapur University, having 15 years of teaching experience, now serving as Associate Professor in MAE Alandi Pune, Maharashtra, India. Research areas of interest are Network Security, Computer Networking, Image processing and Biometric Cryptography.

Sujata Edekar received Bachelor Degree of Engineering in Computer Technology from Nagpur University & pursuing post graduate degree in Computer Engineering from MAE Alandi Pune University, having 5 years of teaching experience, now serving as Professor in BSIOTR (W),Pune. Research areas of interest are Network Security ,Computer Networks.