UGC Approved Journal

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified

Vol. 4, Issue 6, June 2017

A Review on Covert Timing Channels & their Applications

Mandeep Kaur[1], Harsimranjeet Singh[2]

ECE Dept., GIMET, Global Institute of Management & Emerging Technologies[1,2]

Abstract: Covert network timing channels control time between transmissions of packets in overt network communication and transmits hidden messages. This paper presents an overview of different concepts of covert timing channels such as types, features and properties. There is range of terms used for security of information such as encryption, covert channels, network steganography or information hiding in network protocols. Information is hided into network protocols in case of covert channel, but information is hided into content in case of steganography. Different applications such as VoIP, SSH use covert timing channels for the purpose of security. In earlier days, encryption was only the parameter used for security; so information was not secure however simply using encryption does not prevent detection of communication patterns, so various techniques are developed. The main properties of covert timing channels are undetectability and robustness. Unauthorized access from criminals, hackers & terrorists is avoided by using covert timing channels etc. But there are some negativities of covert timing channels, e.g. terrorists misuse covert channels to coordinate their actions. This paper also discusses about use of covert timing channels and types along with applications and problems occur in covert timing channels.

Keywords: Covert Timing Channels, Security, Typesof covert channels.

1. INTRODUCTION

Today in the world of communication e.g. VoIP, Skype, IMO etc. are applications required reliable secure & undetectable transmission of data. In network covert timing channels secret information transfers is by modification of timing properties of network traffic [1]. To transfer information in different applications the timing and ordering of events are changed in covert timing channels. Some aspects of system behavior are changed and manipulated over time to transfer information, here in this case information is received by system behavior such as in case of password hacking . An unauthorized user can access the data by knowing the transmission time of data, when data is transmitted between parties sender and receiver [2]. In earlier days of communication, encryption was used for the purpose of security but encryption only prevents unauthorized parties from decoding the information. For the security of communication only encryption is not sufficient as a result various techniques are developed to overcome these problems. There are various methods to exhibit the information from some communication system, e.g. an increased message frequency, starts transferring of events. Most securely and carefully designed computer systems may contain covert channels between specific users/processes of different security levels. Some definitions for covert channels according to different authors are following:

- According to Lampson, "a covert communication channel is covert not designed to transfer original information".
- According to Schaefer, "A covert communication channel describe resource state and use that state to transfer information".
- According to Kemmerer, "Covert channels use entities to transfer information from one subject to another".

These definitions are helpful to understand the concept of covert channels. The covert channels can be classified according to various parameters such as active, passive and timing and storage channels. According to source of network connection, timing channels are of two types active & passive. Active channels have separate channels to transfer data; its throughput is higher than passive channels. Passive channels, use existing connection to transfer data; it means additional connection is not required [3]. The most common mechanism behind covert communication is that detection of information is not possible. Packet networks communicate through packet contents and their headers. Hence, the inter packet timings provides a side channel for covert communication in covert timing channel. Figure 1 shows the timing covert channels between sender and receiver.

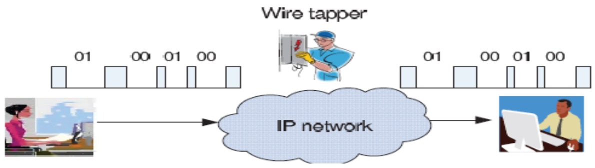

Fig. 1. Covert Communication: An eavesdropper is unable to decode messages modulated by packet timings [4].

The eavesdropper wants to access the packets but fails to access the information packet timings. Covert communication way to transfer information changes such as recently a host of new security applications have arisen where it is desired to communicate - not by means of packets contents – but by utilizing the inter packet timings With advancement in technology.

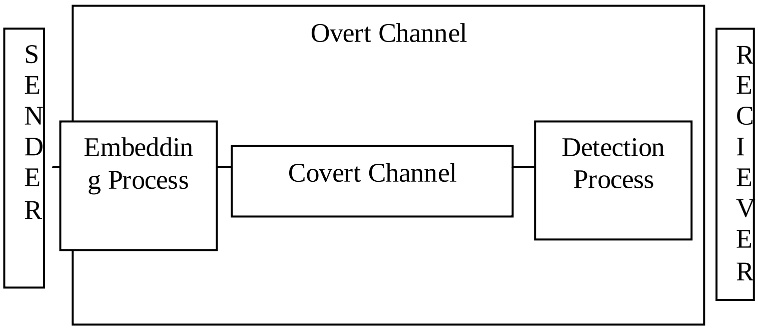

Fig. 2 Covert Communication in Overt Channel

Secure systems are designed by system designers by using set of assumptions and to break the security of that system by violating these assumptions. This principle is clearly defined by covert channel attack where sender and receiver can communicate by manipulating shared resources in unintended way such as in case of side channel attack e.g., timing information, electromagnetic leaks`. Attackers can use such mechanism to leak information, so understanding of covert channel is necessary to improve cyber security. Covert channels are of various types according to their functionalities and utilities such as covert timing channels, covert storage channels, hybrid channels and network based channels. Network based covert channels can exploit unused or non-sensitive fields of network packets (e.g., time to live or IP options) protocol options and properties (e.g., route updates or splitting algorithms) or timing of packets (inter-arrival time or jitter) to transmit bits of data covertly. There is another category of covert channel that is hybrid channel which is combination of two or more communication channel. Generally in covert channel there are three mechanisms send, receive and feedback mechanism. The hybrid channel may have a send mechanism which uses network and receive mechanism that uses operating system. A variety of mechanisms are used in modern computers to transmit timing and storage information. Most studies focus on network channels that can send or receive information over the network. Additionally, hardware devices, such as PCI peripherals, are shared among processes within a computer and can be used to transmit covert data. Moreover, operating systems maintain large amounts of data about the system and contain many data structures that can potentially be manipulated [5]. Covert communication is that in which characteristics and resources of a communication medium used to send secret information. The main requirement of secure communication is needed in internet. Several diverse methods of using exploiting this communication medium for hidden information exchange purposes are introduced. Accomplishment of covert communication based on the specific technique that how this covert communication is accomplished, it can be classified into three major categories. There are various methods of covert communication in networks but among them the simplest and most straightforward methods of covert communication in networks is to utilize specific header fields of the overt network packets that are not used for regular communication and their information is substitute with covert data. The covert storage channel is establish a covert channel based on different protocols Session Initiation Protocol (SIP) signaling during the signaling phase of Voice-over-IP (VoIP). The main utilization of covert communication is in applications such as IMO, Skype and banking transactions etc. Another type of covert channel is covert timing channel in which transfers a covert “1” by sending a packet during a given time interval and a covert “0” by not sending a network packet. Jitter Bug is another method that is known as the Jitter Bug covert channel, where during a network terminal session the transmitted keystroke timing is manipulated by applying delays to the corresponding packets this delay is important for proper reception of data. The efficiency of covert channels depends on different parameters and features. The following are the features of covert channels:

- Impact on covert channel
- Covert channel capacity
- Covert channel bit error rate
- Network delay
- Network jitter
- Desynchronization between covert sender and receiver
- Packet loss
- Capacity and Latency
- Reliability

DOI10.17148/IARJSET.2017.4632

These are the factors with the help of which efficiency of covert channel is determined[6]. The covert channel should not be observable to any monitoring system. The main importance of covert channels is in computer networks. Heterogeneous structure of communication networks combined with relatively high data rates make computer networks an appealing setting for covert channels. The existence of covert channel should be hided. The main characteristics of covert channels are undetectable and robustness and covert rate. There are number of methods that are designed to detect, eliminate, limit or enhance the capacity of network covert channels. The following are the characteristics of covert channels:

- Undetectability
- Robustness
- Covert Rate

Undetectability means channel should not be detectable to some monitoring system. This means that covert channel must be measureable by the intended recipient only. Existence of a file or time used for a computation, have been the medium through which a covert channel communicates but this should be hided from unauthorized access in normal communication of data. But covert channels are not easy to find because these media are so numerous and frequently used. Access control mechanisms are used to hide covert channels as a covert channel is hidden from the access control mechanisms of ultra-high-assurance secure operating system, since it does not use the legitimate (original information) data transfer mechanism of the computer systems, and therefore cannot be detected or controlled by hardware based security mechanisms therefore these channels are named as covert channels means hidden channels. Covert channels are not easy to install in real systems as the data is numerous. A covert time is undetectable according to some statistical test, if the test cannot distinguish between legitimate and covert traffic as the covert timing should be undetectable.

Robustness is a property of covert channel which is use to handle delay or error during transmission. So robustness should be increased by enhancing various parameters and goal in designing a robust covert channel is to deal with the network noise (e.g., network jitter), and by introducing additional noise into the channel (i.e., jamming) prevent active adversaries from disrupting the covert channel. In fact, it is shown that adding random delays into inter-packet delays of the overt traffic can effectively diminish the throughput of timing covert channels in communication networks. In advance communication systems the covert message is directly merged into the Inter-Packet Delays (i.e., IPD) of the overt (original information) traffic.

The another property of covert channel is covert rate. The covert rate is defined as exchange rate of covert information between covert sender and receiver. The covert rate should be as high as possible. Thus, these three characteristics robustness, undetectability and covert rate are used to measure the performance of covert channels [7].

2. CLASSIFICATION OF COVERT CHANNELS

A covert channel is a path that can be used to transfer information in a way not intended by the system’s designer. There are various types of covert channel attack and a covert channel is a type of computer security attack that creates a capability to transfer information objects between processes that are not supposed to be allowed to communicate by computer security policy this is merged into original information. Covert channels can be classified into two categories;

- Covert Storage Channels
- Covert Timing Channels

2.1 Covert Storage Channels

CSC is used to transfer information through the setting of bits by one program and the reading of those bits by another. What distinguishes this case from that the bits are used to convey encoded information. CSC occurs when out-of-band data is stored in messages for the purpose of memory reuse. Steganography, concealing information in such a manner that no one but intended recipient knows of the existence of the message, is a good example of CSC. In CSC 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 involved. Storage channels use memory locations, such as object attributes, its existence and shared resources (input and output devices), for transmission of data.

2.1.1 Classification of Covert Storage Channels

CSC are classified two channels, these are entity attributes and shared resources. These are defined as following:

- Entity Attributes: In entity attributes, for storage channels file name can be used, so this method is quite different. This is utilized between two or more processes and it can be changed by one process. When a read operation performed by any other process a message transfer between the processes occurs. File attributes, which contains properties about a file, can also be manipulated. Even if we are asking for a file which does not exist, the feedback status returned by file system can be used for storage channels.

DOI10.17148/IARJSET.2017.4632

- Shared Resources: Whereas in shared resources as disk blocks, physical memory, I/O buffers, allocated I/O devices, and various queues for shared devices, such as printers and plotters. These methods and devices can be used as storage channels.

2.2 Covert Timing Channels

A timing channel is one type of a covert channel for passing unauthorized information. In this way, one process signals information to another process by modulating its own use of system resources channel for passing unauthorized information. The timing channel passes information by using the speed at which things happen for example a phone call. The main aspect of CTC is time because CTC convey information by modulating some aspect of system behavior over time, so that the program receiving the information can observe system behavior and protect information. Some examples of CTC are system's paging rate, the time certain transaction requires to execute for example in banking, and the time it takes to gain access to a shared channel. CTC can tunnel through secure operating system and require special measure and techniques to control these channels. CTC can communicate through existence of a file or time used a computation. CTC are not easy to find because these media are so numerous and frequently used.

Current Implementations of covert channels are:

- IPV4
- IPV6
- DNS
- HTTP
- MSN
- ICMP
- VoIP

A potential covert channel is a timing channel if its scenario of use involves a process that "signals information to another by manipulating 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."

2.2.1 Classification of Timing Channels

CTC can be classified according to network connection used. These are of two types active and passive channels are as following:

- Passive: In passive channels, no additional connection for communication is required. An existing connection established by the user to transfer covert data therefore possibility of detection is less than active channels. Some statistical tests are used to distinguish covert traffic and legitimate (original) traffic.
- Active: Timing channels that spawn a separate connection to transfer covert data. They are capable of achieving significantly higher throughput as compared to passive timing channels. As the attacker has to create his own connection they are more prone to detection.

3. Evaluation Creteria

- Capacity: Capacity is measured in bits per second in channel. But for network covert channels it can be measured in bits per overt packet. Maximum error free transmission rate can be determined from capacity.
- Robustness: means to handle with delay or error during transmission & determines how easily capacity of covert channel is limited by channel noise.
- Stealth: It tells about detectability of covert channels. determines how easily a covert channel can be detected by comparing the characteristics of traffic with covert channel and unmodified legitimate traffic.

4. Effect of Noise on covert channels

Noise is the main problem that occurs in covert timing channels and noise corrupts data signals and information rate also be reduced. Communication channels are of two types, noisy or noiseless. Noise increases the error rates in a communication channel. The capacity of a channel is its maximum possible error-free information rate in bits per second. By using error-correcting codes, the error rates of noisy channels can be reduced[3].

5. There are various techniques and methods used for security of information by using various methods. Some of them are presenting below:

- Steganography: This technique use codes to write information. This coding may be called as ciphering. This is used in cryptography, such as in cryptography the information is accessible to persons who have key. This key is only shared between sender and receiver.
- Information hiding: is method to prevent accessibility of some aspects of software components form its clients. The term encapsulation is used in information hiding and interchangeably used in place of it.

DOI10.17148/IARJSET.2017.4632

- Encryption: This method is also used for secure communication used in cryptography. In this technique, information is encoded in such a way so that it cannot be accessed by the unauthorized parties.
-

6. Types of data which can be secure by using these timing channels:

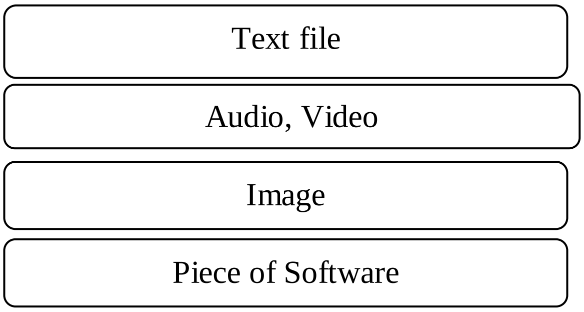

Fig. 3 Utilization of covert timing channels

7. Purpose of covert timing channels:

- Penetration test of firewall/IPS/Proxy
- Secure communication over ad-hoc network

3. CONCLUSION

In this paper we introduce covert channels. What is the utility of covert channels? Need of covert channels in secure communication & types of covert channels? The covert channels used in different applications for the purpose of security e.g., VoIP and Skype etc. This paper gives an overview on covert channels. Covert network timing channels transmits hidden messages by controlling time between transmissions of packets in overt network communication. The main properties of covert timing channels are undetectability and robustness. Covert timing channels are used to avoid unauthorized access from criminals, hackers & terrorists etc. But there are some disadvantages of covert timing channels, e.g. terrorists use covert channels to coordinate their actions. This paper also discusses about applications of covert timing channels.

REFERENCES

[1] G. Liu, J. Zhai, and Y. Dai, “Network covert timing channel with distribution matching,” Telecommun. Syst., vol. 49, no. 2, pp. 199–205, Feb. 2012.

[2] S. Gianvecchio, H. Wang, D. Wijesekera, and S. Jajodia, “Model-based covert timing channels: Automated modeling and evasion,” in Proc. Symp. Adv, Intrusion Detection., 2008, pp. 211–230.

[3] Nitish. Salwan, Sandip Singh, Suket Arora, Amarpreet Singh “An Insight to Covert Channels” in Proc. Symp. Adv, Cryptography and security., 10 June 2013, pp. 311-320.

[4] N. Kiyavash and T. Coleman. “Covert timing channels codes for communication over interactive traffic,” in Proc. IEEE Int.

[5] Hamed Okhravi, Stanlay Bak, Samuel T. King “Design, Implementation and Evaluation of Covert Channel Attacks.” In Proc. Symp. Adv, Covert Channel Attacks, 2010, pp.360-370.

[6] Rezaei, Fahimeh; Hempel, Michael; Shrestha, Pradhumna Lal; and Sharif, Hamid, "Achieving Robustness and Capacity Gains in Covert Timing Channels" (2014). Faculty Publications from the department of Electrical and Computer Engineering. Paper 307.

[7] S.A. Ahmadzadeh and G. Agnew, “Turbo Covert Channel: An iterative framework for covert communication over data networks.” In Proc. IEEE Conf. Comput. Commun. (InfoCom), Apr. 2013, pp. 2031-2039.