International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-4, Issue-2, March 2106

A Covert Channel Using Secret Splitting

Dr. Abdulameer Khalaf Hussain

***Abstract*— This paper presents a design of a secure covert channel . The proposed system generates a special covert channel used in sensitive applications. In order to enhance the covert of information, the participants in the communication channel must agree upon secure information and split it into two parts. From each part, the system generates a set of pseudo random numbers. Then the authenticated users select one of these numbers to be meaningful message. The system depends on the traditional prisoner's problem. The proposed system is tested against the traditional methods and it is implemented more effective in terms of hiding information from the observation of any active warden.**

***Index Terms*— Covert Channel, Information Hiding, Secret Splitting, Timing Attacks.**

I. INTRODUCTION

Covert channel was first introduced by Lampson [1] for secret information transmission. Taking network protocols as carriers, covert channel has recently been widely applied for covert communication on networks. Network covert channel [2, 3] hides the secret communication into normal network traffic to resist detection. Through network covert channels, government agencies, criminals, and terrorist organizations communicate secretly while hackers send out malicious commands. Hence, designing hard-to-detect network covert channels are very important to secret information transmission.

There are many notable methods to design network covert channel. One important branch is to use packet length. Padlipsky [2] and Girling [3] proposed to use the length of link layer frames directly. Yao [4] proposed another covert channel called LAWB based on the packet length. Such covert channels based on packet length could enhance tamper resistance. However, they are still vulnerable to detections due to the abnormal network traffic.

Often covert channel is thought that the use of encryption is sufficient to secure communication. However, encryption only prevents unauthorized parties from decoding the communication. In many cases the simple existence of communication or changes in communication patterns, such as an increased message frequency, are enough to raise suspicion and reveal the onset of events. Covert channels aim to hide the very existence of the communication. Typically, covert channels use means of communication not normally intended to be used for communication, making them quite elusive [5].

Manuscript received October 15,2016

Dr.Abdulameer Khalaf Hussain, Associate Professor , Computer Department, Jerash/ College/ Faculty of Information Technology, Jerash, Jordan,Mobile No 00962796799969.,

While a serious threat even for single hosts, the potential for covert channels in computer networks is greatly increased. In computer networks overt channels, such as network protocols, are used as carriers for covert channels [6,3].

Covert channels in computer network protocols are similar to techniques for hiding information in audio, visual or textual content (steganography). While steganography requires some form of content as cover, covert channels require some network protocol as carrier. The ubiquitous presence of a small number of network protocols suitable as carriers (e.g. the Internet Protocol [8]) make covert channels widely available.

Network administrators can use covert channels to secure network management related communication by hiding it from hackers [9]. Again this is not strong security in the cryptographic sense. Honeypots, which are computer systems set up as trap for hackers, can also use covert channels to export logged data in real-time hidden from the attacker [10].

When we take about covert channels, the prisoner problem is important basic for hiding information . The prisoner problem was first posed by Simmons and is the de-facto model for covert channel communication [11]. Two people, Alice and Bob,1 are thrown into prison and intend to escape. To agree on an escape plan they need to communicate but Wendy the warden monitors all their messages. If Wendy finds any signs of suspicious messages she will place Alice and Bob into solitary confinement — making it impossible for them to escape. Alice and Bob must exchange innocuous messages containing hidden information that (hopefully) Wendy will not notice. Craver describes the different types of wardens [12]:

-A passive warden can only spy on the channel but cannot alter any messages.

-An active warden is able to slightly modify the messages, but without altering the semantic context.

-A malicious warden may alter the messages without impunity, but in reality malicious wardens are rare [12].

There are different types of covert channels. The first type is storage channels which are methods of communication that “include all vehicles that would allow the direct or indirect writing of a storage location by one process and the direct or indirect reading of it by another” [13].

The second type is timing channels which are methods of communication that “include all vehicles that would allow one process to signal information to another process by modulating its own use of system resources in such a way that the change in response time observed by the second process would provide information” [13]. The third type is noise in covert channels**.** One of the major problems in a successful implementation of a covert channel is noise. “A noisy channel intentionally or accidentally corrupts the data

signal with errors so that the information rate is slower than the data rate" [14].

Steganography is a method of covert communication that relates well to covert channels. It is any method used to conceal a secret object within another public object [15]. When employing any steganographic techniques, a cover-file is used to hide the information. It can be a text-file, audio, image, video, piece of software, or others [16]. A common example of steganography is known as least significant bit (LSB) insertion. In a 24-bit bitmap image, the colors red, green, and blue have one byte each that represent their intensities. A steganographer could replace the least intense bits with the hidden message. If done correctly, this should not alter the image enough to be noticeable to the human eye. However, the more data stored in the picture, the more the picture is altered [17].

II. RELATED WORKS

In [18] the authors designs a covert channel depending on event channels .Covert channel between virtual machines is one of serious threats to cloud computing, since it will break the isolation of guest OSs. Even if a lot of work has been done to resist covert channels, new covert channels still emerge in various manners. In this paper, we introduce event channel mechanism in detail. Then we develop a covert channel called CCECS(Covert Channel using Event Channel State) and implement it on Xen hypervisor. Finally we quantitatively evaluate CCECS and discuss the possible mitigation methods. Results show that it can achieve larger bit rate than most existing covert channels.

In [19] a new, plausible deniability approach to store sensitive information on a cluster-based file system had been proposed. Under the proposed approach, a covert channel is used to encode the sensitive information by modifying the fragmentation patterns in the cluster distribution of an existing file. As opposed to existing schemes, the proposed covert channel does not require storage of *any* additional information on the file system. Moreover, the channel provides two-fold plausible deniability so that an investigator without the key cannot prove the presence of hidden information.

Song Li investigated a covert channel implemented on top of MAC protocols that are based on splitting algorithms. Covert information is embedded in nodes' splitting decisions. The covert channel can operate in three modes. The conservative mode is the safest in the sense that use of the covert channel is undetectable. The aggressive mode generates best throughput, but is more vulnerable to detection. A strategic mode is also available which allows the covert users to make a tradeoff between delectability and covert capacity. Simulation shows that the covert throughput ranges from 0 to as high as 0.3 bits per slot, depending on various parameters. It is easy to implement and very difficult to detect [20].

Known covert channel based on splitting algorithms in Medium Access Control (MAC) protocols requires the receiver's knowledge of the sender's identity. In [21] the authors presented a new covert channel that does not have this restriction. In such a channel, multiple senders may operate independently without knowing each other, and the receiver can learn the transmitted information without knowing the identity of any covert sender a priori. These properties make the channel robust to malfunctioning senders, and more importantly help protect the secrecy of senders' identity which is essential for covert communications. The authors also analyze the capacity of our proposed covert channel.

III. PROPOSED SYSTEN

In this paper, we design a different type of a covert channel using two concepts, first splitting a secure information to segments and secondly generating pseudo random number to hide information in the covert channel and then deceive the warden.

The whole information will be split into two classes C_0 and C_1 . Then the proposed system generates a pseudo random number in such a way that the generation is governed by a strict secure method to deceive the warden. The authenticated users will choose one meaningful piece selected from wide pieces generated as a pseudo numbers. Figure 1 illustrates the general system design.

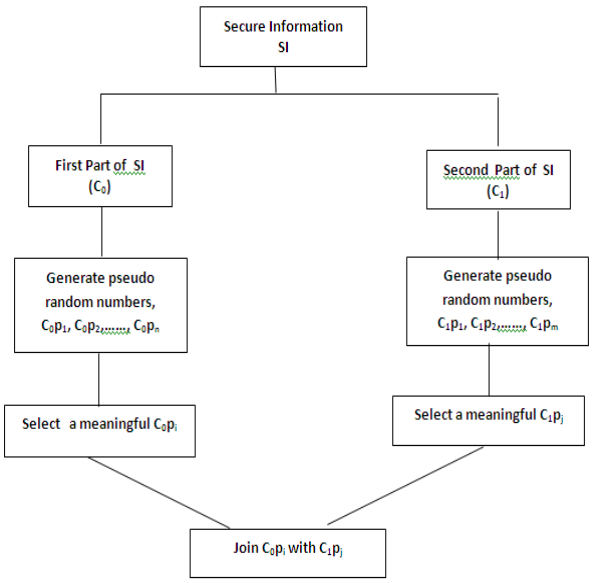

Fig 1: General System Design

The method of choosing a meaningful piece of information from pseudo numbers depends on two techniques. The first one is the agreement in advance among authenticated users about that piece. The second technique is by using the k-nearest piece of different parameters characterized by the previous piece. In other words the users can choose the meaningful piece from the property of the previous one such as its security strength in the first trial and the amount of information of the previous one. So if we apply the first technique we use a secure piece of information as an agreement parameter. If we suppose the number of pieces of pseudo numbers is C0n and the number of pieces of pseudo numbers is C_{1m} then the agreement parameter is determined by taken the ith one from C_0 and the jth item from C_1 , the agreement is $i*j+(i_2*j_3)$ mod $(L_1 + L_2)$ where L_1 is the length of the first segment of pseudo numbers and L_2 is the length of the second segment of pseudo numbers.

In the second technique we use the K-nearest of the next suitable piece of information. If we suppose the ith segment is characterized by the parameters such as the ith length (Lp) , the location in the whole information (Loc) , then the next nearest piece is (Lp(ith)+Lp(ith+1))/2 ad the nearest location of the next piece is Shift(3)(Loc(ith)). So

the next piece is characterized by properties different to the previous and thus we add more security and provide a strong method of deceiving the attacker.

IV. CONCLUSION

In order to hide information of covert channels, this paper proposes using secret splitting which is considered a strong method to enhance both secrecy and authenticity. The strength of this covert channel comes from the agreement by the authenticated parties upon secure information and then splitting it into two parts. From each part we use the generation of pseudo random number. These numbers are much more secure than real random numbers. So, the participants in the communication will be able to select a hidden piece that cannot be discovered by any active warden. Thus the authenticated parties can get two meaningful piece of information that can not be estimated by any observer in the communication.

The system also uses the concept of nearest neighbor to select a meaningful message from each part of the splitting information .The concept of nearest neighbor can generate more hidden meaningful messages So this system proposed two alternative technique to agree upon the meaningful messages.

REFERENCES

[1] B. Lampson, "A note on the confinement problem", Commun. ACM, vol. 16, no. 10, Oct. 1973, pp. 613–15.
[2] 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, Mitre Corporation, August 1978.
[3] C. G. Girling, "Covert channels in LAN's", IEEE Trans. Software Engineering, vol. SE-13, no. 2, Feb. 1987, pp. 292–96.
[4] Q. YAO and P. ZHANG, "Coverting channel based on packet length", vol.34 No.3 Computer Engineering, February 2008.
[5] B. Lampson, "A Note on the Confinement Problem," Commun.ACM, vol. 16, no. 10, Oct. 1973, pp. 613–15.
[6] 6] 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, Mitre Corporation, August 1978.
[7] J. Postel, "Internet Protocol," RFC 0791, IETF, Sept. 1981. http://www.ietf.org/rfc/rfc0791.txt.
[8] [8] D. V. Forte *et al.*, "SecSyslog: An Approach to Secure Logging Based on Covert Channels," *Proc. First Int'l. Wksp. Systematic Approaches to Digital Forensic Engineering*, Nov. 2005, pp. 248–63.
[9] The Honeynet Project, "Know Your Enemy: Sebek — A Kernel Based Data Capture Tool," tech. rep., 2003, http://www.honeynet.org/papers/sebek.pdf.
[10] G. J. Simmons, "The Prisoners' Problem and the Subliminal Channel," Proc. Advances in Cryptology (CRYPTO), 1983, pp. 51–67.
[11] S. Craver, "On Public-Key Steganography in the Presence of an Active Warden," Proc. 2nd Int'l. Wksp. Information Hiding, Apr. 1998, pp. 355–68.
[12] Department of Defense. Trusted Computer System Evaluation Criteria, 1985.
[13] N. Proctor and P. Neumann. Architectural Implications of Covert Channels. SRI International, 1992.
[14] M. Owens. A Discussion of Covert Channels and Steganography." SANS Institute, 2002.
[15] K. Reiland. Steganography and Covert Channels. PACISE conference. Bloomsburg, PA, 2005.
[16] G. Kessler. Steganography: Hiding Data Within Data. 2001.
[17] S. Qingni , W.Mian ,Z. Zhuangzhuang , Z. Zhi , Q. Sihan and W. Zhonghai ," A Covert Channel Using Event Channel State on Xen Hypervisor" , Proceeding of ICICS 2013 15th International Conference on Information and Communications Security - Volume 8233 , Pages 125-134 , 2013.
[18] K. Hassan , J. Mobin , A. Syed , and M. Fauzan ," Designing a cluster-based covert channel to evade disk investigation and forensics" , Computers & Security , Volume 30, Issue 1, January 2011, Pages 35–49.
[19] L. Song , "A covert channel in MAC protocols based on splitting algorithms" , Wireless Communications and Networking Conference, 2005 IEEE (Volume:2).
[20] W. Zhenghong , and R. Lee, , "Mutual Anonymous Communications: A New Covert Channel Based on Splitting Tree MAC" , INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE , 2007.

Dr. Abdulameer K. Husain, Jerash University- Jordan. He has completed Master degree in computer science ,university of Sadam , Iraq , in 1991 and his PhD thesis in computer science , computer security from Al- Neelain University ,Sudan . He has total 20 years teaching experience and presently working as Associate professor in Jerash University – Jordan.

