SECURITY APPROACH FOR COMPUTER NETWORK BASED ON DETECTING COVERT CHANNEL IN TCP/IP PROTOCOL

By

Mr. Borhade Ajit M.
ME Information Technology 2nd,
AVCOE, Sangamner
+91 9021976600

Prof. Borkar Bharat S.
Assistant Professor,
Department of Information Technology
AVCOE Sangamner
+91 9822579911

ABSTRACT:

A covert channel is any methodology of communication that's accustomed illicitly transfer data, so breaking the protection policy of the system. Any shared resource will probably be used as a covert channel. There are several threats that fashionable network security should take under consideration. From brute force watchword attacks to port scanning, the issues, that system engineers and administrators should worry regarding, increase at a quicker than traditional pace. However, one in all the problems that several within the field haven't paid enough attention to is covert channels. During this paper, we have a tendency to gift an outline of covert channels with examples. We have a tendency to explore the 2 forms of covert channels: storage channels and temporal order channels. Storage channels are additional normally used than timing channels as a result of their easier to implement each represent major security threats. Covert channels are often designed for either one system or a network. It's necessary for system engineers to know covert channels in order that they're going to be able to preemptively overcome sure security issues.

Keywords: *Covert Channel, Storage Channel, Timing Channel, Steganography, Security and Network.*

ISSN: 2278 – 1323

I.INTRODUCTION

Until the Eighties, problems with network security seldom entered into the minds of system engineers that has all modified. A system's security currently has prime priority. Despite this reality, several system programmers have unnoticed the threat of covert channels. Though they need been around since the dawn of contemporary computing, they're solely currently getting down to receive wider attention. Parenthetically the matter additional totally, allows us to use associate analogy. Alice and Bob are incarcerated and placed in 2 separate jail cells. They require coordinating associate escape set up. However, they need a little drawback. All messages that they send to every different should 1st be browse by the peace officer before being passed on. so as to be able to coordinate their plans whereas at an equivalent time keeping them hidden from the peace officer, they convey with one another in code. Every word with an excellent variety of letters is browse as a one. Every word with associate odd variety of letters is browse as a zero. as an example, if Bob sent a message to Alice asking "Hey, what area unit you up to," Alice would interpret is as "010011." The peace officer, during this case, has been used as a covert channel [1]. Though no prisoners would most likely try that in reality, it works alright as associate analogy for a way a covert channel operates. A covert channel is any channel that may be exploited by a method to transfer in-formation in an exceedingly manner that violates the system's security policy [2]. There are a unit 2 differing kinds of covert channels, called covert storage channels and covert temporal arrangement channels, severally. Following this introduction, we tend to in short discuss storage channels, temporal arrangement channels.

II.COVERT CHANNEL

In this section, we discuss the basics of covert storage channels and covert timing channels, with examples of each..

2.1 Storage Channels

Covert storage channels are strategies of communication that "include all vehicles that might permit the direct or indirect writing of a storage location by one method and also the direct or indirect reading of it by another [2].In alternative words, one method writes to a shared resource, whereas another method reads from it. Storage channels are often used between processes among one pc or between multiple computers across a network [3]. A decent example of a storage channel could be a printing queue. The method with higher security privileges, the causing method, either fills up the printer queue to signal a one or leaves it because it is to signal a zero. The method with lower security privileges, the receiving method, polls the printer queue to envision whether or not or not it's full and deter-mines the worth consequently.

Figure 1: Example Storage Channels

2.2. Timing Channels

Covert temporal order channels area unit ways of communication that "include all vehicles that might enable one method to sig-

ISSN: 2278 – 1323

nal in-formation to a different method by modulating its own use of system resources in such the way that the amendment in latent period ob-served by the second method would offer information" [2]. In alternative words, it's primarily any technique that uses a clock of your time to signal the worth being sent over channel. Equally to storage channels, temporal order channels will exist each during a single-computer setting and a network setting. However, they're less sensible during a network setting [4].

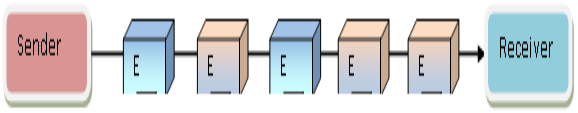

Figure 2: Example Timing Channels

III.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-delectability is doubtful.

LAN Environment Covert Channels

Girling [3] first consider network covert channels. He concentrated on local area networks 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 [8], 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

ISSN: 2278 – 1323

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.

IV. PROPOSED SYSTEM

The use of pseudorandom number generators has been widely spread when producing ISNs. PRNGs generate a sequence of numbers that approximate the properties of random numbers. Thus, the sequence is not truly random. The randomness of ISNs makes attackers hard to predict these numbers; the idea not to use truly random numbers for ISNs lies in that if a connection arrives, the randomness of ISNs would make it uncertain that the coming sequence number would be different from a previous incarnation. The PRNG old by the Windows wince cryptogram is the most commonly used PRNG. The pseudorandomness of the vintage of this generator is exquisite for the anchor of involving Harry fascinate dynamic in Windows. The PRNG is modeled as a function whose input is a short random seed, and whose output is indistinguishable from truly random bits. Implementations of pseudorandom number generators often use a state whose initial value is a random seed. The state is updated by an algorithm which changes the state and outputs pseudorandom bits, and implements a deterministic function of the state of the generator. To analyze this chaotic/nonlinear behavior, we turn to phase space reconstruction method, which is a useful chaotic/nonlinear signal processing technique. This method to build a spoofing set in predicting ISNs generated by Windows 2000. Some weaknesses of the Windows PRNG were revealed.

Phase Space Reconstruction

Chaos can be defined as a random and no uniform phenomenon in the deterministic nonlinear system and hidden discipline in a complex system can be revealed by chaos theory. Chaos theory makes people aware that often there are certain laws behind the seemly random phenomena. With conventional tools such as Fourier transform, chaos looks like “noise”, but chaos has structure seen in the phase space. Phase space reconstruction is the first step in nonlinear time series analysis of data from chaotic systems. It is a useful nonlinear/chaotic signal processing technique to characterize dynamic system, whether low-dimensional or high-dimensional. Reconstructed phase spaces have been proven to be topologically equivalent to the original system and therefore are capable of recovering the nonlinear dynamics of the generating system. This implies that the fully dynamics of the system are accessible in this space, and for this reason, a phase space reconstruction and features extracted from it can contain more

ISSN: 2278 – 1323

and/or different information than a spectral representation. Phase space reconstruction consists of viewing a time series $X_k = X(k\tau), k = 1,2....N$ in a Euclidean space R^m where m the embedding dimension and τ is the sampling time. By doing this we expect that the points in R^m form an attractor that preserves the topological properties of the original unknown attractor. Here, an attractor is a set towards which a dynamical system evolves over time. Geometrically, an attractor can be a point, a curve, a manifold, or even a complicated set with a fractal structure known as a strange attractor. According to this concept, a dynamic system can be described by a phase space diagram, which is essentially a coordinate system, whose coordinates are all the variables that are necessary to completely describe the state of the system at any moment. Among a variety of methods available for phase space reconstruction, the method called "delayed coordinates" is well known and widely used. This method is based on the concept that we can reconstruct missing dimension using its previous and delayed function values as coordinates. A given time series, $X_i, i = 1,2,3,....N,$ can be reconstructed in a multidimensional phase space to represent the underlying dynamics according to:

$$Y_j = (X_j, X_{j-\tau},..., X_{j-2\tau},.., X_{j-(m-1)\tau}) \qquad (1)$$

Where $j = 1,2,..N-(m-1)$ and m is the dimension of the vector Y_j, also called as embedding dimension, and τ is the delay time. Further expand we have:

$$Y = [Y_1, Y_2,..., Y_j,.., Y_m] \qquad (2)$$

Where Y_j is the vector of m dimension an M is the number of vectors in this multidimensional phase space. M Can be given by $M = N-(m-1)$ .Based on the chaos theory the vector fully represents the nonlinear dynamics when m is large enough. A correct phase space construction in a dimension m facilitates an interpretation of the underlying dynamics. The physics behind such a reconstruction is that a nonlinear system is characterized by self-interaction, so that a time series of a single variable can carry the information about the dynamics of the entire multiple-variable system.To reveal the hidden structure of ISNs the phase space can be constructed by using "delayed coordinates". For a given sequence of $ISN(i)$ numbers, the phase space is constructed as follows:

$$Y_i = (ISN(i), ISN(i-1),.., ISN(i-(m-1))) \qquad (3)$$

Where $i = 1,2,..N-m+1, N$ is the number of ISNs and m is the dimension. Vectors Y_i in the new phase space are formed from time delayed values of the scalar measurements. Used phase space reconstruction to build a spoofing set in predicting ISNs. Instead of using delayed coordinates, the first-order difference for the input data is used in the phase space construction. This method shows patterns of the correlation within a set of 32-bit ISNs generated by several operating systems' PRNG. By using "first-order difference" as the coordinates the phase space is constructed as follows:

$$\begin{aligned} x(n) &= ISN(n) - ISN(n-1) \\ y(n) &= ISN(n-1) - ISN(n-2) \\ z(n) &= ISN(n-2) - ISN(n-3) \end{aligned} \qquad (4)$$

ISSN: 2278 – 1323

This is a three-dimensional representation of one-dimensional input data. Here $x(n)$, $y(n)$ and $z(n)$ are called points coordinates.

The PRM Model

A phase space is created by establishing vectors in R^m. According to the chaos theory, phase vectors can fully represent the nonlinear dynamics if the embedding dimension *m* is large enough. There are various methods to estimate the *m* including empirical methods. Different values of such as 2, 3, 4, 5 and 6 were tested in creating the reconstructed phase space as shown below, and *m*=4,5 and 6 gave us 100% detection accuracy rate. The larger the, the higher the computational complexity is. So *m*=4 is selected. The coordinates of four-dimensional vector are calculated as follows:

$$\begin{aligned} x(n) &= ISN(n) - ISN(n-1) \\ y(n) &= ISN(n-1) - ISN(n-2) \\ z(n) &= ISN(n-2) - ISN(n-3) \\ w(n) &= ISN(n-3) - ISN(n-4) \end{aligned} \quad (5)$$

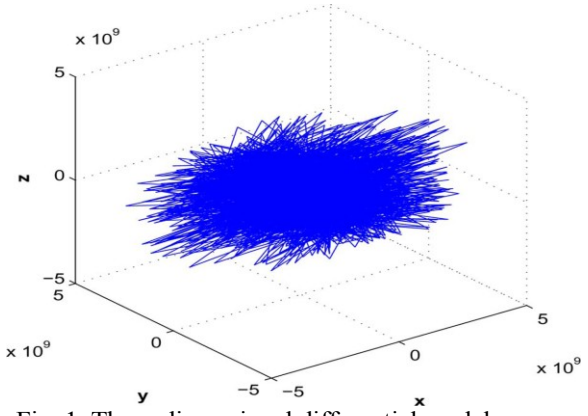

Fig. 1. Three-dimensional differential model.

Where $n = N, N-1, N-2, \ldots 5$ and N is the number of ISNs. The four–dimensional phase vector r_i is constructed as:

$$r_i = [x(i), y(i), z(i), w(i)], i = 1,2,\ldots M, M = N-5 \quad (6)$$

Let us use *R* to represent the phase space or dataset formed by the (5) and (6). If the number of ISNs is *N*, the number of phase vectors or elements in the phase space *R* is *N-5*, each is a four-dimensional vector.

$$R = [r_1, r_2, \ldots . r_M] \quad (7)$$

As shown by Fig. 1, these vectors in phase space have some level of relations. In order to extract features from the dataset *R* , we define distance between any two vectors r_1 ,r_2 in the phase space *R* as:

$$d_{ij} = \sqrt{(x(i)-x(j))2+(y(i)-y(i))2} \times \sqrt{(z(i)-z(j))2+(w(i)-w(j))2}$$

Proposed Classification Algorithm

The statistical model is constructed by legally generated ISNs. In our experiment we used a dataset of 745 ISNs which are collected by using Win Dump for Windows XP SP3 operating system. Half of these is used to construct the statistical model in the four-dimensional phase space, and then to obtain the third-order feature of the proposed statistical model. The other half is used for testing. The stego-ISNs are generated by the algorithm Covert_TCP, in which ISN field is replaced with actual ASCII character to be encoded. The encoding of ASCII codeword of letter H is performed by the 72 256 65536. Here, the ASCII code for character H is 72 (Hex). This enables a more realistic looking sequence number. Using this method, that packet is sent to the destination host. The destination host, expecting to receive information from client, simply grabs

ISSN: 2278 – 1323

the ISN field of each coming packet to reconstruct the encoded data. This way of encoding secret message in ISNs has been tested in application and is considered a practical breakthrough to hide information in ISNs.

V. CONCLUSION

In this paper, we have given an overview of covert channels in computer network protocols. We have given review of different mechanism for creating and detecting covert storage and covert timing channels. There are number of protocols that can be used as carriers to make covert storage channel. We also describe the modules that are used to detect covert channel in TCP/IP protocol. Our research will continue with further study in developing covert channel detection and defences.

REFERENCES

[1] Hong Zhao, Senior Member, IEEE, and Yun-Qing Shi, Fellow, IEEE," Detecting Covert Channels in Computer Networks Based on Chaos Theory", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 2, FEBRUARY 2013

[2] M. McFail. Covert Storage Channels: A Brief Overview. *PACISE conference.* Bloomsburg, PA, 2005.

[3] Prof. RajeswariGoudar, SujataEdekar," Ephemeral Feature Presentation of Covert Channels in Network Protocols", International Journal of Scientific and Research Publications, Volume 3, Issue 6, June 2013.

[4] M. Owens. A Discussion of Covert Channels and Steganography." SANS Institute, 2002.

[5] K. Reiland. Steganography and Covert Channels. *PACISE conference*. Bloomsburg, PA, 2005.

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

[7] Nishant D. Rohankar, A. V. Deorankar, Dr. P. N. Chatur," A Review of Literature on Design and Detection of Network Covert Channel", International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 1, Issue 2, November 2012.

[8] 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

ISSN: 2278 – 1323