AN EFFECTIVE COVERT TIMING CHANNELS DETECTION: SUPPORT VECTOR MACHINE & HYPERBOLIC HOPFIELD NEURAL NETWORK

G. Yuvaraj¹, S. John Paul²

¹(Dept. of CSE, PG Scholar, Sri Venkateswara Institute of Science and Technology, Thiruvallur, gyuvarajdce@gmail.com)
²(Dept. of CSE, Asst Professor, Sri Venkateswara Institute of Science and Tech., Thiruvallur, johnpaul.svist@gmail.com)

Abstract—A network covert channel is a mechanism that can be used to leak information across a network in violation of a security policy and in a manner that can be difficult to detect. Detecting and preventing covert channels is particularly important for multilevel security systems in which processes working with classified information may leak information to processes with a lower classification level via the use of shared resources. A lot of generic mechanism that can be used to detect a large variety of covert channels. However, those mechanisms have more limitation like speed of detection, detection accuracy etc. In this project, a novel machine learning approach called Support Vector Machine and Hyperbolic Hopfield Neural Network is used to classify the covert channels data packets. The proposed approach is categorized into two phases such as Support Vector Machine Training and Convert Channel prediction. Finally, we shown the proposed method is an effective approach to detect the covert channels from the shared network resources.

Keywords— Covert Channels; Detection; Machine Learning; Traffic Fingerprints

1. INTRODUCTION

Covert channels provide methods to transmit information using existing system resources that were not designed to carry data. This makes them invisible to common network security mechanisms like firewalls. Because of their ability to evade detection, they create a grave cyber security threat. Sensitive and confidential information can be leaked from a network with higher security privileges to an external network by simply establishing a seemingly innocuous communication link between them. Two parties with intention to covert data can easily communicate and exchange information over a public network without being detected.

Therefore, it is very difficult to detect covert communications and this can be a very effective and damaging security approach if it is used for harmful intentions. There are two countermeasure approaches to covert communications. One approach is using a network monitoring entity called a network warden that modifies all traffic passing through it regardless of whether it is covert or not. This is called active warden approach.

This modification of the underlying traffic may possibly make it impossible for the receiver to decode the hidden message. However, doing so will unfairly punish innocuous traffic as well, often leading to waste of computing resources.

An active modification of traffic may not be possible without violating the QoS provisions in the network, particularly in applications where the order of packets and the timing requirements of them are tightly guided by the communication protocol. Therefore, a passive warden approach which can detect presence of covert message in the traffic is required. Such approaches will investigate the traffic and set up alarms, and take corrective measures upon detection of covert messages in a particular stream.

A Support Vector Machine (SVM)-based detection framework that can blindly detect Covert Timing Channels (CTCs). CTCs are a class of covert channels that embed bits into traffic by modulating the timing information of the traffic. The presented framework uses statistical fingerprints generated from the traffic under investigation as the feature point vectors to train a Support Vector Machine-based classifier. In this paper, we have derived four types of statistical fingerprints from the timing information of the traffic being tested—Kolmorov-Smirnov (K-S) score, Regularity score, Entropy and Corrected Conditional Entropy (CCE).

The hidden bits are embedded within the timing information, building a detector based on the statistical fingerprints derived from the timing information itself will correlate well with the presence of such covert bits.

We show that the framework is generic and does not require any information of the embedding process, and can accurately detect the presence of the CTCs. A novel machine learning approach called Support Vector Machine and Hyperbolic Hopfield Neural Network is used to classify the covert and overt channels data packets. The proposed approach is categorized into two phases such as Support Vector Machine Training and Convert Channel prediction. Finally, we shown the proposed method is an effective approach to detect the covert channels from the shared network resources. Here, a new machine learning neural network approach called Hyperbolic Hopfield is used to improve the covert channels prediction in the shared network resources.
2. RELATED WORK

Covert channel is different from cryptography as its main aim is to hide the existence of transmission whereas cryptography does not hide the existence of message but transform it in a form that is only readable by receiver. In cryptography there is no intention to hide the communication. Covert channel in computer network protocols and steganography are closely related but often confused. Steganography involves hiding of information in audio, visual, or textual content. While steganography requires some form of content as a cover, covert channel requires some network protocol as a carrier.

The network covert channels are communication channels that are not designed nor intended to exist, the communication streams must be embedded inside authorized channels. They may be based on existing protocols from OSI low layers (e.g.: IP, TCP, UDP) to OSI high layers (e.g.: HTTP, SMTP). The general idea of covert channels relies on the idea that information can be transferred in redundant or unused fields of network protocols.

Network security analysts first started thinking about covert channel communication, two terms have been introduced, storage and timing covert channels. In storage covert channel, one of the processes directly or indirectly writes to a particular storage location whereas other process reads from that location.

Number of tools employs TCP, IP, ICMP, and HTTP protocols to establish storage covert channels. In these protocols unused fields are used to transmit the information. In a way steganography can be seen as a form of storage covert channel.

The timing covert channel involves modifying the time characteristics to hide information. Specifically it can be done by modulating inter-packet delays. We pay our attention to detect covert channels related to TCP ISN and IP ID fields. At the SVM training time they collected normal TCP/IP packets using a tcp dump tool and abnormal TCP/IP packets(including covert fields) generated from covert tcp and then tested it for IP Identification field of IP header and sequence number field of TCP header.

The works on network timing channels can be traced back to the point in that temporal covert channels .Some network timing channels require time synchronization between encoder and decoder. Our proposed a timing channel where one bit is conveyed through transmitting data or not and Cabuket applied a similar idea to IP packets. To transmit a ‘1’, the trojan visits a dynamically4 determined group of cache sets (G1) andreplaces all of the constituent cache blocks, and for a ‘0’ it visits another dynamically determined group of cache sets (G0) and replaces all of the constituent cache blocks. The spy infers the transmitted bits as follows: It replaces all of the cache blocks in G1 and G0, and times the accesses to the G1 and G0 sets separately.

If the accesses to G1 sets take longer than the G0 sets (that is, all of the G1 sets resulted in cache misses and G0 sets were cache hits), then the spy infers ‘1’. Otherwise, if the accesses to G0 sets take longer than the G1 sets (that is, all of the G0 sets resulted in cache misses and G1 sets were cache hits), then the spy infers a ‘0’. But we are using in hyperbolic Hopfield neural network approaches technique used in our proposed system. This system is used to training and testing dataset from extraction data in database and its transmit detection dataset to prediction results.

3. SYSTEM DESIGN

Figure 1 shows the block-diagram representation of the detection framework. The detector is essentially network monitor that has access to all traffic it is attempting to investigate. It could either be implemented to pass all network traffic through it as shown in figure, or it could simply tap into the traffic stream. It consists of three primary units—a traffic filter, a fingerprint extractor and a SVM framework. The traffic filter selects traffic for fingerprint extraction. This is a circular problem with no solution.

Furthermore, we have shown in that the use of these fingerprints fails when the size of the embedded covert message is small. In, the authors extended the work of Gianvecchio et al. By introducing two additional fingerprints for detecting CTCs—the K-L divergence and Welch’s t-test.
They show that the Welch’s t-test is better suited to detect the Jitterbug algorithm’s as it is a non-parametric test based on difference of means. An SVM based machine learning approach that uses there gularity metrics as the feature points has also been proposed. But this classifier has been tested against only one CTC. In the authors have successfully used the SVM classifier techniques for classifying specific CSCs. The authors discuss covert channels that use TCP/IP header fields such as IP Identification and Sequence Number, and ICMP payload traffic and detect them using a SVM based pattern classifier. But they cannot be readily extended to incorporate CTCs as well.

4. CONCLUSION

Currently available detection methods are designed to detect a very specific type of covert channels, and the detection principle cannot be extended to incorporate more channels. Furthermore, they lack the requirement of blind detection and scalability. A novel machine learning approach called Support Vector Machine and Hyperbolic Hopfield Neural Network is used to classify the covert and over channels data packets. The proposed approach is categorized into two phases such as Support Vector Machine Training and Convert Channel prediction. Finally, we show the proposed method is an effective method to detect the covert channels from the shared network resources.

REFERENCES