covert channel

by Sapna V M

Conference Paper Title*

Ghanashyam Mahesh Bhat
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address

Karan Bhat Sumbly
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address

Kumkum Geervani
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address

Prajwal Bhat
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address

Dr. Sapna V M
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address

Abstract—This document talks about various covert channel classes, their detection and prevention schemes.

Index Terms—covert channel, machine learning, malware, data exfiltration, network, detection, prevention, dataset

I. INTRODUCTION

A covert channel is a communication channel to obscure information sharing between hosts and circumvents existing security barriers. The fleeting headway in computing power provides new opportunities in expanding the use of covert channel communications for malware exfiltration of data, orchestrating nodes of a botnet, or sending remote commands[2] while avoiding getting detected by firewalls, intrusion detection systems, and anti-viruses [11]. Although covert channels can be used for achieving sound objectives like implementing digital watermarking in VoIP traffic, developing traceback techniques, or avoiding censorship, in reality, it is being used for criminal activities making them a threat to cybersecurity [12]. Covert channels pose a serious risk to the privacy and security of the systems as it goes mostly undetected because of the least generalizability and scalability of the covert channel detection and analysis tools [2]. The issue arises from the fact that there are indefinite ways to conceal information in a covert channel and the tools developed can only address certain types of covert channels. This paper sheds light on the details pertaining to the various types of covert channels and techniques for the detection of the same along with some approaches that can be used to hinder covert communication.

II. COVERT CHANNEL CLASSES

There are mainly three classes of Covert channels namely: 1)Storage channels 2)Timing channels 3)Hyper channels[1].

Covert channels are also classified based on information flow sequences, entropy analysis and patterns according to Pattern Language Markup Language[5].

A. Storage Channels

Storage channels use a principle of concealing information in the header fields of the protocols. This can result in amending the packet structure, altering the padding bits, or re-arranging optional fields[6]. In these channels, a shared storage location will be used as a channel to conduct secret messages. A sender uses this shared location directly or indirectly to write a message and the receiver utilizes this shared location directly or indirectly to read the messages[3].

B. Timing Channels

In timing covert channels, the covert message is modulated into the timing behavior of an entity[1].In timing covert channels, a sender exploits a system re-score aspect to signal a secret message, and then, the receiver observes and decodes the secret message. A covert message is modulated into the timing behavior of an entity[3]. Timing channels conceal information by using timing properties of network traffic – mainly IAT[6].

C. Hyper Channels

A hyper-covert channel is a concept that combines both storage and timing channels. Storage channels have an upper hand in providing high bandwidth whereas timing channels prove hard to be detected[3]. Hyper channels integrate both these advantages, hence detection of hyper channels is very laborious.

Even though we classified covert channels into only three main categories, there are actually numerous ways to create a covert channel. The first release of CCgen tool for the injection of the covert channel itself provides multiple ways of injecting covert channels into real-world traffic[12]. The diversity of covert channels makes it difficult to generalize the solution to detect covert communication effectively while making sure that it doesn't add much overhead to the network[13].

III. DATASET GENERATION

The most common approach to solving problems due to covert channels is using machine learning techniques, which require a large volume of data for training the model[10]. Obtaining public network traffic for testing covert channel detection is challenging and there are no public datasets available[1]. Hence we make use of tools that help in generating datasets. pcapStego is a tool used for creating network covert channels within .pcap files[10]. It aids in the creation of large datasets containing real network traces[10]. targeting Flow Labels, Traffic class, and Hop Limit. The tool allows the creation of channels We can see that data which consists of real TCP traffic taken from the LBNL/ISI Enterprise Tracing Project[5] is used. A dataset with 4-bit and 8-bit symbol channels is created for testing. An example includes traffic collected on an OC192 link in different conditions made available by the Center for Applied Internet Data Analysis (CAIDA)[6]. The real network data downloaded from MAWI working group traffic is another use case seen. The dataset generated by the tool is better than other toy datasets[10]. Collecting the data from real traffic for the purpose of research is not ethical since the data in a real-world network will be private and may contain sensitive information[10]. Thus making it necessary to generate our own dataset with the help of the existing tool which mimics real-world traffic.

IV. ANALYSIS OF COVERT CHANNELS

There are various analysis techniques available for covert channels. Analysis methods must be fast and lightweight. In DAT detectors[5], Multimodality and the Sum of Autocorrelation coefficients are used.

- Multimodality - 1) Uses Kernel density distributions for the estimations using Pareto charts. Processes for estimating multimodality seek to find the number of statistical modes contained in a population, that is, the number of significant peaks displayed by the probability density function of a random variable.
  2) Symbols using Pareto Charts - to find the number of symbols that occur the most using Pareto analysis.
- Sum of Auto-correlation coefficients - Covert channels have a greater probability of being detected by this method.

Graphical Analysis of covert channel patterns is most commonly seen. Inter-field analysis uses a set of patterns obtained from ML classifiers during offline analysis. It considers combinations of OD-flow vector values in different TCP/IP header fields[5].
A set of customized rules and thresholds are defined for every specific field according to the expected distribution characteristics, field type, and value ranges done in intrafield analysis. It also helps in checking TCP/IP header fields separately by examining the corresponding OD-flow vector values[3]. Sensitivity analysis is one such method helpful in detecting storage channels. Tools like Wireshark are used for the analysis of packets flowing over a network[7].

bccStego is a high-throughput tool for measuring general statistics of the packets[11] where the state is neglected in order to achieve lesser memory usage and minimal overhead. This tool can be integrated with other frameworks to design the detection scheme with less overhead to the network. bccStego makes use of BPF and it can be extended to measure different aspects of the packets as per the requirement. Once the data is collected, the presence of the covert channel can be detected by analyzing the variation in the bin size[11].

V. DETECTION SCHEMES

The switching techniques assist in developing a covert channel that is hard to detect[3]. Internal control protocol technique that provides a reliable and trusted communication channel for a covert message[3] increases the use of these channels.
Challenges faced during the covert channel detections include: a) Noisy Channels b) Covert channels in address fields and bouncing covert channels c) Covert channels modeled according to field distribution properties d) Covert channels with encrypted messages. Storage channels provide high bandwidth and timing channels are hard to detect[3]. Hybrid covert channels pose a real challenge in detection since they are a combination of storage and time channels.
We can use DAT detectors, various Machine Learning approaches,etc.
Covert channel Detection techniques can be classified as:

- Value to Symbol correspondence - usually detected by the intra-field analysis. The context abstraction is compared with references of expected or non-suspicious distributions, which are ultimately shaped by a set of rules and thresholds[5].
- Value range as Symbols - similar to Value to symbol correspondence but the number of multimodality distribution peaks is more than the number of multimodality symbols[5].
- Container fields - The intra-field analysis block is mainly addressed to checking container fields in the IP and TCP options fields. They can be detected using packet compliance checks [5].
- Timing Channel - can be considered as value ranges as symbols for the packet IAT field[5].
- Derivative Approaches - detected using the sum of auto-correlation coefficients and mean differences[5].

Detection methodologies in Passive Warden Scenario can be grouped into[5]:

- Traffic irregularities – Packet Compliance Checking Phase
- Statistical Analysis – Multimodality, Autocorrelation, Descriptive Statistics
- Machine Learning – Inter-field Analysis(Offline Analysis)

Detection of Storage Covert Channels includes:

- Detection of Channels Targeting the Flow Label
- Sensitivity Analysis

- Channels Targeting other Ipv6 fields[5]

Sensitivity analysis includes three attack scenarios[6]:
a) Exfiltration attempt modeled via transmission of file requiring to target 8500 Ipv6 packets.
b) Different channels alter in time.
c) APT targeting datacenter or subnetwork.

With the help of a dataset, one can devise a machine learning model to detect covert communication and thus assist in taking actions to prevent the same. SVM has shown a significant result in detecting covert channels over other algorithms, though the statistical variations between the covert channels and overt channels must be clear[1].
With the fast-growing technology and a wide scope for covert channel generation, the machine learning model has to be retrained periodically to detect advanced covert channels[1].

VI. PREVENTION SCHEMES

Based on the literature we have surveyed on covert channels, we were able to devise some techniques that could be effective against network covert channel communication.

A. Timing Channels

In [Decision Tree paper reference], the authors shed light on various timing techniques that can be used for network covert communication.

- Packet presence Technique: This technique requires synchronicity between the sender and the receiver, who agree on a fixed interval as sampling time. The absence or presence of a packet during an interval represents the binary symbol 0 or 1 respectively.
- Fixed intervals: This technique establishes fixed packets' inter-departure times (idts) to represent 0s and 1s.
- Jitterbug: The Jitterbug manipulates an existing transmission. It establishes a ground sampling time interval, let's say X, and adds a little delay to idts to make them divisible by X or $X/2$ according to the covert symbol to send.
- Huffman encoding: This technique codes every covert symbol directly into a set of packets with different idts according to the frequency of the symbol and based on a Huffman codification.
- One threshold: Devised for Android platforms and with video services as carriers, this technique establishes a threshold X for packet inter-arrival times (iats). Delays above and below X will be considered 1s and 0s respectively.
- Packet bursts: By this technique, packet bursts are sent separated by a waiting time interval t. The number of packets in a burst directly represents the covert symbol or piece of code to send.
- Differential/derivative: Given a basic idt, whenever a 1 is to be sent the previous idt is modified by adding or subtracting t_{inc} in case of a 0, the last idt is kept the same, i.e., with no modification.

All the above-mentioned timing channel techniques can be potentially disrupted by adding a random buffer/ delay to the packets by the network router. Apart from those mentioned above, one other timing technique as mentioned in [Decision Tree paper reference] is:

- Timestamp manipulation: By this technique, packet idts are manipulated based on the least significant bit (LSB) of the TCP timestamp. A minimum idt between packets must be respected (authors propose, at least, tb = 10ms). If the LSB coincides with the covert symbol, the packet is sent; if not, the condition is checked again after a time $t_w ait$. This technique can be countered if we configure the router in a way that increments/ decrements the last 3-4 bits of the timestamp field of the packet headers. However, this random change in timestamp must be synchronized with other packets of the same logical connection.

VII. CONCLUSION

We have seen that the covert channel is the reason for multiple privacy and security concerns and there is a need for effective detection and prevention mechanism to counter the attacks using covert channels.

REFERENCES

[1] Muawia A. Elsadig, Ahmed Gafar, "Covert Channel Detection: Machine Learning Approaches," vol 10, pp. 38391-38405, 2022.
[2] Marco Zuppelli, Luca Caviglione, Wojciech Mazurczyk, Andreas Schaffhauser, Matteo Repetto, "Code Augmentation for Detecting Covert Channels Targeting the IPv6 FLow Label," 2021, pp. 450-456.
[3] Muawia A. Elsadig, Yahia A. Fadlalla, "Packet Length Covert Channel: A Detection Scheme," 2021 pp. 1-7.
[4] Arti Dua, Vinita Jindal, Punam Bedi, "Covert Communication using Address Resolution Protocol Broadcast Request Messages," 2021, pp. 1-6.
[5] Félix Iglesias, Robert Annessi, T. Zseby, "DAT detectors: uncovering TCP/IP covert channels by descriptive analytics," 2016, pp. 3011-3029.
[6] Marco Zuppelli, Matteo Repetto, Andreas Schaffhause, Wojciech Mazurczyk, "Code Layering for the Detection of Network Covert Channels in Agentless Systems", vol. 19, no. 3, pp. 2282- 2294, 2022.
[7] Punam Bedi, Arti Dua, "ARPNetSteg: Network Steganography Using Address Resolution Protocol," vol. 66, no. 4, pp. 671-677, 2020.
[8] Félix Iglesias, Valentin Bernhardt, Robert Annessi, Tanjab Zseby, "Decision Tree Rule Induction for Detecting Covert Timing Channels in TCP/IP Traffic," *1st International Cross-Domain Conference for Machine Learning and Knowledge Extraction(CD-MAKE)*, pp. 105-122, Aug 2017.
[9] Muawia A. Elsadig, Yahia A. Fadlalla, "Network Protocol Covert Channels: Countermeasures Techniques," 2017.
[10] Marco Zuppelli, Luca Caviglione, "pcapStego: A Tool for Generating Traffic Traces for Experimenting with Network

Covert Channels," 2021.

[11] Matteo Repetto, Luca Caviglione, Marco Zuppelli, "bcc-stego: A Framework for Investigating Network Covert Channels," 2021.

[12] Félix Iglesias, Fares Meghdouri, Robert Annessi, Tanja Zseby, "CCgen: Injecting Covert Channels into Network Traffic," 2022, pp. 1-11.

[13] Marco Zuppelli, Luca Caviglione, Matteo Repetto, "Detecting Covert Channels Through Code Augmentation," 2021.

covert channel

1	**dokumen.pub** Internet Source	**11**%
2	**onlinelibrary.wiley.com** Internet Source	**10**%
3	Muawia A. Elsadig, Yahia A. Fadlalla. "Packet Length Covert Channel: A Detection Scheme", 2018 1st International Conference on Computer Applications & Information Security (ICCAIS), 2018 Publication	**4**%
4	Submitted to South University of Science and Technology of China Student Paper	**3**%
5	link.springer.com Internet Source	**2**%
6	Marco Zuppelli, Matteo Repetto, Andreas Schaffhauser, Wojciech Mazurczyk, Luca Caviglione. "Code Layering for the Detection of Network Covert Channels in Agentless	**2**%

Systems", IEEE Transactions on Network and Service Management, 2022
Publication

7   Iglesias, Felix, Robert Annessi, and Tanja Zseby. "DAT detectors: uncovering TCP/IP covert channels by descriptive analytics : DAT detectors: uncovering TCP/IP covert channels by descriptive analytics", Security and Communication Networks, 2016.
Publication   1 %

8   Muawia A. Elsadig, Ahmed Gafar. "Covert Channel Detection: Machine Learning Approaches", IEEE Access, 2022
Publication   1 %

9   www.annessi.net
Internet Source   1 %

10   www.coursehero.com
Internet Source   1 %

11   Marco Zuppelli, Luca Caviglione. "pcapStego: A Tool for Generating Traffic Traces for Experimenting with Network Covert Channels", The 16th International Conference on Availability, Reliability and Security, 2021
Publication   1 %

12   ipfs.io
Internet Source   1 %

13 Nadya El Moussaid, Maryam El Azhari. "Enhance the security properties and information flow control", International Journal of Electronic Business, 2020
Publication

<1 %

14 etd.lib.metu.edu.tr
Internet Source

<1 %

15 "Machine Learning and Knowledge Extraction", Springer Science and Business Media LLC, 2017
Publication

<1 %

Exclude quotes	On	Exclude matches	< 5 words
Exclude bibliography	On		