Proc. of the Intl. Conference on Advances in Information Processing and Communication Technology - IPCT 2016.
Copyright © Institute of Research Engineers and Doctors. All rights reserved.
ISBN: 978-1-63248-099-6 doi: 10.15224/ 978-1-63248-099-6-71

Survey on Covert Storage Channel in Computer Network Protocols: Detection and Mitigation Techniques

Muawia A. Elsadig, Yahia A. Fadlalla

***Abstract*— Due to the rapid growth in number of different protocols over the internet, internet protocols have become an ideal vehicle for covert communications. They represent a high bandwidth for such communications. Moreover, new high-speed network technology has significantly amplified the network's covert channel capacity. Certainly, a covert channel bandwidth of only one bit size can easily allow transmission of a system bin code which can lead to tremendous risk. This paper presents a brief overview of network protocols-based covert channels, and surveys some recent and relevant work on covert channels detection and elimination techniques along with their achievements and limitations. In sum, the covert channel countermeasures—detection, elimination, mitigation, and capacity reduction—are still real challenges and lag behind an acceptable level of network security. Therefore, the research door is wide open for more contributions in this field.**

***Keywords*— covert channel, security; detection, prevention, elimination, capacity reduction, network protocols.**

I. Introduction

The rapid development of computer networks and intrusion detection systems (IDS) has led hackers to find new ways to leak or steal confidential information without being detected. A network covert channel is a possible and good opportunity to do this. A network covert channel is a communication channel that permits the transfer of information between two processes on the network in a manner that breaks up the system's security policy [1].

A covert channel allows individuals to communicate in an undetectable manner to exchange hidden information. This explains why detection of covert communication is considered a big issue that faces security systems. Moreover, covert channels are not only used for the exchange of hidden information but could be exploited to pass malicious messages [2], Trojans, viruses, etc. in ways that couldn't be detected by common firewalls or detection systems. A covert channel is classified as a serious threat when combined with such malicious activities.

Commonly, it is known that covert channels cannot be fully eliminated [3, 4]. But there is a possibility that they could be reduced through careful analysis and design[2].

A covert channel may exist in two scenarios: a stand-alone system or a networked-based system. In the case of the stand-alone system, the covert information is passed between entities. In a network–based system, the covert information is transferred over the network [5]. Initially, the research community focused on so-called local covert channels, in which two processes with different security levels can communicate with each other in order to leak information. Typically, a high security level process leaks information to another process possessing a low security level. With the rise and rapid development of computer networks, the focus has been shifted to network covert channels in which covert information can be encoded into network protocols [6].

A covert channel does not always represent a threat; it may be used as a kind of steganography to hide secret messages (i.e., a network administrator may secure the network management communications by using a covert channel to keep them protected against hackers' attacks)[7]. Also, it can be used to transmit secret information such as secret keys [1]. Furthermore, Qian et al. point out that the technology of covert channels has become a novel method for some security approaches such as copyright protection, network authentication, cybercrime evidence, etc.[8]. More works on using covert channel in concept of security purpose can be seen in [9-13].

Covert channels in network protocols look similar to steganography techniques. Both use a carrier to send a covert message, although the nature of the carrier is different. In the case of steganography techniques, information is hidden in a carrier such as an image, video, text, sound, etc., known as an unstructured carrier. In the network covert channel, a network protocol is used as a carrier; this is known as a structured carrier[14, 15]. This type of network covert channel is classified as storage covert channel.

Due to the TCP/IP protocol suite features, it is apparent that most of the recent popular covert channels are constructed based on packet-switching data networks [15]. In addition, traffic encryption as a traditional security measure is promoting the design of different types of network covert channels [16].

The TCP/IP suite is widely used by most internet applications. It represents the biggest communication channel for overt communications. Numerous methods were developed for covert transmission using TCP/IP headers, and, accordingly, many detection methods have been developed to detect such threats. However, covert messages in both the Initial Sequence Number field (ISN) of the TCP Protocol and the Identifier field (ID) of the IP protocol are hard to detect. Both fields use random values according to their standard requirements [5].

Muawia A. Elsadig
Ph.D. Candidate, College of Computer Science and Information Technology, Sudan University of Science and Technology – SUST. Khartoum, Sudan.

Yahia A. Fadlalla
Lead Consultant/Researcher, InfoSec Consulting, Hamilton, Ontario, Canada.
Adjunct Professor, College of Computer Science and Information Technology, SUST.

As covert techniques are still new, further work and research need to be done regarding detection and prevention. Barroso and Santos discussed the art of covert techniques in protocol data packets. They addressed the fact that new protocols continue to burst, so new covert techniques will continue to grow accordingly. Therefore, data confidentiality may be at risk. Moreover, Barroso and Santos pointed out the importance of developing software security that is capable of analyzing network traffic and presenting an effective mechanism to fight against unauthorized data transmissions [17].

The first section of this paper has introduced network protocol covert channels and given a general overview, definitions, and significant issues concerning them. The rest of the survey paper is organized as follows: Section II illustrates the typical covert channel model, which reflects the general concept of the covert channel scenario. Section III sheds light on covert channel classifications, while Section IV highlights the common countermeasures that are used to counter network covert channels. Subsequently, Section V gives a short introduction to covert channel capacity estimation, while Section VI provides comprehensive study and discussions on related work. Achievements and limitations of many detection and prevention approaches are presented. Finally, conclusions and future work are summed up in Section VII.

II. Typical Covert Channel Model

The typical covert channel scenario can be demonstrated through the prisoners problem introduced in [18] by Simmons

Alice and Bob are two prisoners who wish to communicate with each other in order to plan their escape. But the possible channel that allows communication between them is monitored by a third party called Wendy. If any suspicious information exists in this channel, then Wendy or the warden will place Alice and Bob into solitary confinement so they have no way to exchange any piece of information. Therefore, Alice and Bob must try to hide the exchanged information in a way that is impossible for Wendy to detect, so they can communicate covertly. This scenario can be applied to network covert channels by imagining that the communication between Alice and Bob is over two networked computers [19]. Figure.1 illustrates the covert channel model.

III. Network Covert Channel Classification

Typically, as the classic covert channel, the network covert channel is categorized into two main types: covert storage channels and covert timing channels.

Covert storage channels encompass the processes of encoding covert information into network protocol fields (sender) and retrieving back the covert information (receiver). In covert timing channels, a sender can signal information by manipulating packets, frames, or message timing; the intended receiver then observes and decodes the covert information [6, 15]

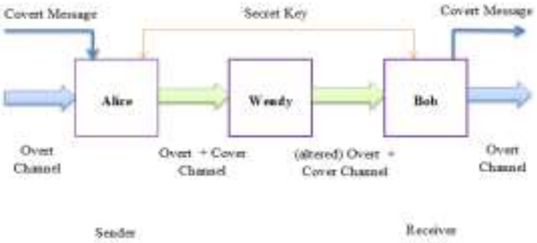

Fig 1: Typical Covert Channel Model [20].

Due to the diversity of the network storage covert channel, Wendzel et al. classify them in two branches: (i) network storage channel methods that hide the covert message in the payload, and (ii) the network storage channel methods that alter non-payload aspects such as header fields [6]. Accordingly, Wendzel et al. classify the non-payload methods into seven patterns, as illustrated in Fig 2. On the other hand, the covert timing channels are classified into four patterns, as illustrated in Fig 3 (overleaf).

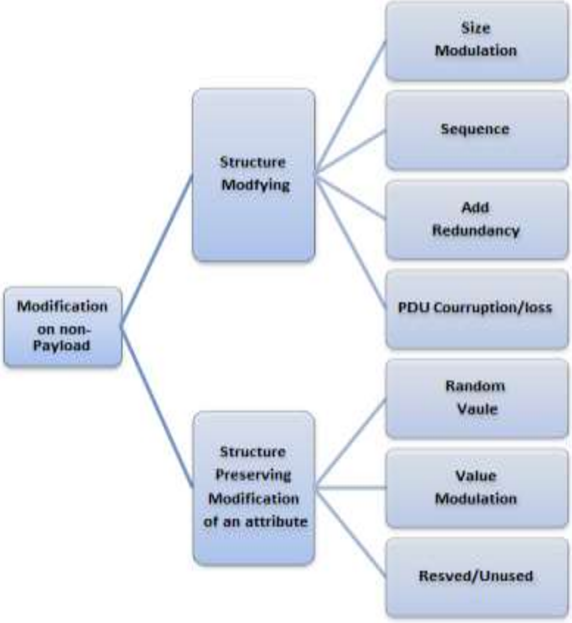

Fig 2: Non-Payload Storage Covert Channel Classifications[6]

Zander et al. introduced another classification for covert channel techniques in network protocols based on their mechanisms. Interested readers are referred to a comprehensive explanation of classification details in [15].

IV. Countermeasures

The depth of knowledge about covert channel techniques is a key to developing countermeasures. Due to the rapid development of computer network communication technology, and its complex nature, it is illogical to look for full elimination of all potential covert channels or to prove their nonexistence. Instead some methods have been developed to lower or degrade the bandwidth of potential covert channels [15]. But, in those cases, a balance should be maintained to keep the overt channel intact and effective while trying to degrade the covert bandwidth. Some common methods for bandwidth reduction or capacity reduction are: introducing noise, setting a fixed size for

Proc. of the Intl. Conference on Advances in Information Processing and Communication Technology - IPCT 2016.
Copyright © Institute of Research Engineers and Doctors. All rights reserved.
ISBN: 978-1-63248-099-6 doi: 10.15224/ 978-1-63248-099-6-71

network packet length, limiting the host to host connections and inserting dummy packets [17].

To apply countermeasures, Zander et al. [15] proposed first identifying the covert channel that is being used and then applying a specific countermeasure. This indicates that a particular countermeasure can be applied after the identification of a potential covert channel.

The countermeasures are grouped into four categories:

a) Eliminating the covert channel (i.e. normalizing protocol headers)

b) Limiting the covert channel bandwidth (i.e. random traffic padding technique)

c) Auditing the covert channel (requires reliable passive warden as a detector)

d) Documenting the covert channel.

Barroso and Santos highlighted the limitations of host security, network security, and traffic normalization when they considered the general approaches for covert channel eliminations [17]. Table 1 shows the approaches and their limitations:

TABLE 1. LIMITATIONS OF SOME ELIMINATION APPROACHES.

Elimination Approach	Limitations
Host Security	It may protect hosts from direct attacks or prevent the channel's exploitation in some situations. However, it cannot remove covert network channels. More details can be seen at [17].
Network Security	It can resist tunneling channels, such as ICMP protocol traffic, but does not address other protocols that can't be blocked.
Traffic normalization	Only simple storage channels can be mitigated.

Most of the proposed detection approaches depend on the recognition of abnormal behavior [21]. Typically, the warden knows the normal traffic behavior in a certain network, so it can easily detect the abnormal behavior that is caused by covert communication. However, if the normal traffic includes considerable variations, then these approaches will fail to detect covert traffic. Moreover, any covert traffic that looks similar to normal traffic will be hard to detect.

V. Covert Channel Capacity Estimation

In covert storage channels, an estimation of the channel capacity can be obtained by the size of the object values. In contrast, in the case of timing covert channels, channel capacity can be estimated by the amount of encodable information in the network resources. Estimation of channel capacity is a key to applying remediation methods used to limit covert channel capacity.

Dye indicates that little work has been conducted on the formal analysis for identifying and measuring covert channel capacity in network protocols [20].

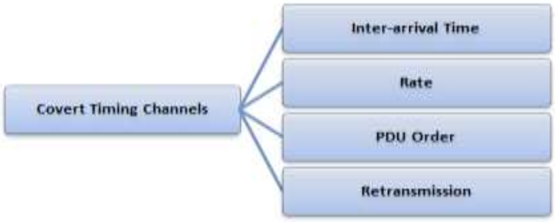

Fig 3: Covert Timing Channel Classifications [6]

VI. Related Work

This section surveys and discusses recent and relevant work on covert channels detection and mitigation techniques along with their achievements and limitations. In addition, this section will focus on covert channel capacity reduction as one of the common mitigation techniques.

Based on Markov model, Zhai proposed a detection algorithm that discovers covert communication in TCP flows. The algorithm has attained good performance in detection of such kinds of covert communications under different applications (i.e. FTP, SSH,HTTP, SMTP, and TELNET) [22]. However, this proposed method is not able to detect covert communications in applications that use tunneling technology rather than TCP ports such as ICMP.

Trying to profile and mitigate covert channel attacks, Gilbert and Bhattacharya proposed a hybrid detection system that combines anomaly-based detection and covert channel profiling [23] . This seeks efficient detection of covert storage channels in computer network protocols by analyzing abnormal traffic. Gilbert and Bhattacharya claimed that their approach is a base for adding new techniques in both fields (abnormal network activity and covert channel research areas).

Dong, Qian, Lu and Lan proposed a network covert channel with construction based on packets classification [24]. It can combine fields from more than one protocol. As the authors explained, their proposed covert channel is too hard to be detected by existing detection systems such as IPS/IDS or Wireshark. Moreover, it can't be totally eliminated.

A signature-based approach is used as a common detection approach to detect network covert channels. The signatures database is built and regularly updated so that when a signature is found within the monitored traffic, the monitoring sensor will trigger an alarm. This approach can effectively distinguish network covert channels from normal traffic. An example of applying this approach in covert channels can be seen in [25]. The drawback of this approach is the inability to detect any covert channel which has not been found before [1].

As mentioned previously, the TCP/IP protocols suite is the heart of the internet. It involves the most protocols that are vulnerable to exploitation by covert channel threats. The covert channel in the Initial Sequence Number (ISN) field of the TCP protocol seems to be the one that is most difficult to detect compared with other fields in the aforementioned protocol, such as reserved and unused fields [26]. Sohn, Seo and Moon proposed a detection method based on a support vector machine (SVM) classification approach to detect ISN

Copyright © Institute of Research Engineers and Doctors. All rights reserved.
ISBN: 978-1-63248-099-6 doi: 10.15224/ 978-1-63248-099-6-71

covert channels [27]. However, their method is too complicated and time consuming. It requires a large number of normal and abnormal ISNs for machine training purposes. In contrast, Zhao and Shi proposed an alternative detection method for ISN covert channels. Their proposal is based on characterizing the dynamic nature of ISNs using phase space reconstruction. They developed a statistical classification model in order to identify the covert information. They claimed that their proposed method performs well in detection of such covert channels with less computational overheads. Moreover, it can be used as an online detection method to examine live network traffic.

Basing their work on trained neural networks, Tumoian and Anikeev developed a detection method for ISN covert channels [28]. Various operating systems produce diverse ISN values, therefore, the training phase is host-dependent. After the completion of the training phase, the neural network is used to evaluate the test traffic. The results show that the false negative rate is ranged between 5% and 10%, while the false positive rate is less than 0.5%.

Murdoch and Lewis developed two covert channel schemes using the TCP\IP ISN field as a carrier [29]. The two schemes are based on encoding data generated by Linux and OpenBSD within the ISN field. In contrast with many other covert methods, their schemes are difficult for wardens to detect, since the ISN data generated by the aforementioned schemes is indistinguishable from the data generated normally by the TCP\IP stack. So, in this case, a warden would be unable to detect the covert channels unless the warden knew the shared secret key.

Hussain et al. proposed a high bandwidth covert channel in network protocol [30]. To avoid detection, they used normal packet length features. Further, to expand the covert channel capacity, they utilized the packet payload as a covert data communication. Their proposed method is time efficient, high capacity, and temper resistant for network traffic detectors. The trend of keeping the covert traffic looking similar to normal traffic behavior is working against detection methods that rely on distinguishing between normal and abnormal traffic. However, in comparison with other techniques, this approach is complicated. Moreover, it utilizes the packet payload—the information content—as a hidden container[16].

Rohankar et al. reviewed some mechanisms that are used to create and detect covert storage and covert timing channels in computer network protocols [31]. They figured out that most of the time, storage channels are preferred to timing channels. In timing channels, synchronization is required between sender and receiver. In addition, Rohankar et al. pointed out that using multiple fields in a given protocol—rather than a single field—for covert communications leads to complicate the detection of such covert channels and it would be a real challenge.

Most detection algorithms and techniques that counter network covert channels focus on a single type of covert channel instead of focusing on the common characteristics of multiple covert channels. Pushing for a way to find out common characteristics or behaviors of network covert channels, Wendzel et al. classified existing covert channel techniques of the period (1987 to 2013) into eleven patterns. These are arranged in a hierarchical catalog using the Pattern Language Markup Language (PLML)[6]. In addition, Wendzel et al. mentioned that around 70% percent of these techniques can be categorized into four main patterns. These findings will assist in developing a common framework that can be used to build up a common detection method that could detect all or most existing covert channels. On the other hand, Yuwen et al. proposed a detection algorithm with clusters based on hierarchy and density [1]. They claimed that their detection method could detect several types of covert channels; moreover, it could work effectively to distinguish between normal traffic and covert traffic, even if the channel noise rate reaches 20%.

Fisk et al. introduced the Minimal Requisite Fidelity (MRF) concept. This is a measure of the accepted degree of signal fidelity to end-users that can destruct covert communications [32]. In other words, this can determine a degree of signal fidelity that can eliminate covert communications without affecting the overt channel productivity. Fisk et al. mainly concentrated on using structured carriers, such as network protocols. They used a specification-based approach to obtain MRF. In contrast, for an unstructured carrier (e.g. image), the technique of adding noise can reduce the channel bandwidth effectively. However, this technique is not suitable for structured carriers, as it affects the overt communications. Fisk et al. claimed that their proposed warden, which is based on the MRF technique, can effectively eliminate covert communications in a structured carrier (network protocol) that has strict semantics. However, the MRF technique was not effective in an unstructured carrier.

IPsec protocol is used to ensure secure communication between different machines. However, this protocol itself could be exploited as a covert channel to leak information from one machine to another. This defeats the essential purpose of this protocol—protecting the overt communication. Kundu indicates that existing approaches to mitigating covert storage channel threats are affecting the usability of many QoS-aware applications. To address this issue, Kundu proposed an approach for mitigating such threats without compromising usability[33].

Basing their work on normalizing incoming and outgoing network packets, Dakhane and Deshmukh proposed an active warden to eliminate covert storage channel traffic [5]. It is only designed to deal with TCP sequence numbers. According to their experimental results, their proposal can successfully eliminate up to 99% of possible covert communications via the TCP sequence number field. It works by limiting or lowering the channel bandwidth.

Lowering covert channel bandwidth or capacity is a method of prevention. This can be accomplished in many ways, such as adding noise to the channel. This method will not eliminate the channel, but it can make it difficult for the channel to accomplish its task [34].

Active wardens can protect against outside attackers and malicious insiders. They have can alter the information flow in order to remove or eliminate the covert content without affecting the overt communications. In addition, active wardens can introduce a bogs message into the covert communications [13]. [16] and [5] are examples of active wardens being used to lower covert channel bandwidth.

Network storage covert channels can be achieved through two techniques [16]: the first is based on

ISBN: 978-1-63248-099-6 doi: 10.15224/ 978-1-63248-099-6-71

modulating packet header fields (such as Type of Service (ToS) [19], Time to live (TTL) [35], Internet Protocol ID [36], etc.); the second is based on packet-length modification. Obviously the bandwidth of the packet-length covert channels is significantly higher than the bandwidth of covert timing channels. Therefore, covert storage channels in networks have received more attention than timing covert channels. It represents a serious threat which can lead to significant security breaches. Epishkina and Kogos proposed a random traffic padding approach to estimate and limit packet-size-based covert channel capacity. Their technique generates and introduces a dummy packet [16].

Commonly, from a security point of view, a covert channel at a low bandwidth is a lesser threat than one at a high bandwidth [37]. However, most of the techniques used to reduce the bandwidth degrade system performance. Therefore, a balance has to be attained between system performance and the rate of reducing covert channel bandwidth. Certainly, a 100 bit per second (bit/s) bandwidth is considered “high bandwidth” as most terminal devices work at this rate. It would not be appropriate to say this computer system is “secure”, as its information is compromised at the same rate of the normal output device’s rate. In multilevel computer systems, bandwidth of 1 bit/s is an acceptable level for reducing the covert channel threat in many applications. However, attaining this level in some applications is impractical. It affects system performance. In such cases, instead of reducing the bandwidth to an exact level, it possible to watch and audit the use of the potential covert channels. This auditing can help to detect and recover from significant impairments.

Fadlalla introduced the spurious processes approach to limit covert storage channels in Multi-level secure (MLS) systems [38] . The objective is to limit covert channels, taking into account the alternation of shared resources. When a normal process, A, tries to access a shared resource that was previously accessed by another normal process, B, a spurious process is introduced to access the shared resource before A. The goal of the spurious process is to introduce a kind of uncertainty to the shared resource status for process A. This way, process A can’t identify which process has modified the shared resource status.

Packet-length covert channels are based on the modulation of a covert message into network packet lengths, so it can be transmitted covertly over the network. Yao et al. developed a packet-length-based covert channel model [39]. In this, the two communicators (sender and receiver) exchange a secret matrix. In the matrix, each cell has a unique length. The sender selects a random length from the matrix to build a payload message with the same length. After obtaining the payload length of the received message, the receiver determines the matching length in the shared matrix and thus obtains the corresponding raw number. This is the scenario for exchanging covert messages through this approach. As the packet lengths are picked from a limited range, the covert traffic cannot precisely imitate normal traffic. This leads to easier detection of such covert channels.

Zhang et al. proposed a covert channel scheme that relies on using packet lengths [40]. The distribution of the lengths of packets generated by their scheme is very close to normal traffic distribution in overt communications. Therefore, their covert scheme is difficult to be detected through algorithms that are based on recognizing abnormal traffic. The authors validated their scheme’s high performance in detection resistance.

Ji et al. developed a message-length-based covert channel, which resists against active detections, for detection approaches based on recognizing abnormal traffic [41] . Their approach relies on using normal network communication traffic as a reference for covert traffic. However, adding the lengths of hidden messages to the reference results in some sort of abnormal traffic. This leads to weakening of this approach’s resistance to detection systems, especially when using large data volume. In the other words, in cases of high volume covert communication, this approach fails to attain sufficient simulation for normal network traffic. This motivated Ji et al. to develop the Normal-Traffic Network Covert Channel (NTNCC) approach, which is also based on message length [42] . As per their claim, the NTNCC attains a great level of resistance against network traffic detections.

Nair et al. highlighted the spread of using packet lengths to hide secret information and the growth of this technique day by day [43]. The existence of numerous applications that are based on sending random sized packets, instead of working with a particular pattern, motivated steganographers to modulate their covert messages into the length of the network packets. This feature is one of the important factors behind developing many steganographic algorithms that exploit network packet length. Accordingly, Nair et al. proposed a network steganalysis scheme capable of detecting such covert communications. To distinguish between normal and stego traffic, their detection scheme uses two-dimensional feature space to train the scheme classifier. As per the authors’ claim, experimental results showed high accuracy. However, no comparison with the other existing schemes is presented, as the authors claim no such detection schemes exist. Moreover, the experimental scenario is only applied to UDP traffic.

Commonly, the straightforward way to eliminate packet-length-based covert channels is to equalize packet lengths to maximum length. However, this technique diminishes overt channel capacity. For an alternative approach, packet length covert channels can be limited by decreasing the possible lengths a packet could have. This limits the covert channel capacity by reducing the number of states a covert message can exploit. In the case that a packet is too small, the packet can be padded with zeroes. However, this approach wastes the overt channel bandwidth[20]. Therefore, an effective solution for reducing or limiting covert channel capacity—without affecting the overt communication capacity—is still a real challenge. Exploring this, Epishkina and Kogos investigated and examined the channel capacity of a given packet-size-based covert channel. Accordingly, they designed a countermeasure tool based on the generation of random traffic padding to limit covert channel bandwidth or capacity [16]. To adjust the parameters of the aforementioned tool, it is first necessary to estimate the covert channel capacity of the covert channel under investigation.

The first covert channel technique that is capable of switching a network protocol is introduced in [44]; this is based on user commands. Recently, new covert channel techniques have been developed; these are based on protocol-switching capabilities. The added value of these

Proc. of the Intl. Conference on Advances in Information Processing and Communication Technology - IPCT 2016.
Copyright © Institute of Research Engineers and Doctors. All rights reserved.
ISBN: 978-1-63248-099-6 doi: 10.15224/ 978-1-63248-099-6-71

techniques is they give a covert channel the ability to switch its communications between different protocols automatically. The lack of countermeasures to address such kinds of covert channels motivated Wendzel and Keller to develop the first approach (as per their claim) based on limiting the bandwidth of protocol-switching covert channels [45]. They introduced a new active warden for this purpose. The usefulness of their technique has been evaluated practically. In their approach, constant delay is introduced to reduce the channel capacity. Wendzel and Keller extended their work by enhancing the active warden to introduce constant and random delay [46]. However, the regular traffic (legitimate traffic) is also affected by this delay. Therefore, the authors suggested combining the active warden with detection functionality, and applying whitelisting based on formal grammar to reduce the amount of delay affecting normal traffic. As the authors stated, this approach was not designed to fit large network environments where redundancy protocols and load balancing are essential.

Recently, covert channel–internal control protocols have been presented to improve network covert channel capabilities. These are called micro protocols. Placing micro protocols within a covert message provides some communication features for covert channels (i.e. dynamic routing, session management, reliable data transfer, etc.). Wendzel and Keller conducted a review paper concerning the micro protocols' general functionality, capabilities, drawbacks, etc. [47]. They pointed out the observable lack of micro-protocols countermeasures. Moreover, Kaur et al. indicated that existing techniques to counter network covert channels are not capable of countering micro protocols. This assumption motivated them to develop and implement countermeasure techniques that effectively counter and break the kind of sophisticated covert communication that utilizes micro protocols [48]. They implemented their countermeasures in two different micro-protocol tools (Ping Tunnel and Smart Covert Channel). Compared to the current mechanisms, the authors claimed that their countermeasures performed better because they mainly targeted the behavior of micro protocols, while existing techniques do not.

Even though numerous approaches have been conducted in the design and implementation of covert channels, many protocols are still vulnerable to delivery of covert data, either for illegitimate or legitimate objectives. Rios et al. evaluated some protocols that have not yet been exploited for such purposes. Particularly, they evaluated DHCP, Bluetooth and NetBIOS protocols. As they claimed, the aforementioned protocols have not yet been used as carriers for covert communications [49]. Based on these findings, the authors developed and implemented a covert channel that exploits DHCP protocol. This is considered the first implementation of covert communication in this protocol.

Garcia et al. shifted the focus towards covert channels that threaten power control systems. They claimed that the existing security schemes in such systems only take into consideration the explicit communications. Based on this claim, Garcia et al. proposed a novel covert communication channel that uses physical substrates of a power system—such as power lines communications—as a carrier of covert messages between compromised devices [50]. It is notable that their approach does not need any explicit communication channels. Therefore, intrusion systems can't recognize these types of covert communications. For future research, the authors will shift their focus to developing a physical-based covert channel detection method for detecting such types of covert communications

VII. Conclusion and Future Work

As covert techniques are still new, further work and research need to be done regarding detection and prevention. New protocols continue to burst, so new covert techniques will continue grow accordingly. Data confidentiality may be at risk.

Most of the proposed detection approaches depend on the recognition of abnormal behavior. Typically, the warden knows the normal traffic behavior in a certain network, so it can easily detect abnormal behavior caused by covert communication. However, if the normal traffic includes considerable variations, then these approaches fail to detect covert traffic. Moreover, any covert traffic that looks similar to normal traffic will be difficult to detect.

On the other hand, most of the detection algorithms and techniques that counter network covert channels are focused on a single type of covert channel, rather than the common characteristics of multiple covert channels. In the fact, some attention has been paid to this issue, and some work in this direction has been done, but more in-depth work is still required to enrich the contributions in this direction. The success of this will assist to develop common security policies to fight against network covert channel threats.

Deep knowledge of covert channel techniques is a key to developing covert channels countermeasures. Due to the rapid development of computer network communication technology, and its complex nature, it is illogical to look for full elimination of all potential covert channels or to prove their nonexistence. More work in alternative solutions—such as reducing covert bandwidth, auditing covert channels, documenting covert channels, etc.—is urgently required. Moreover, in the case of bandwidth reduction, the solution should keep the regular traffic capacity intact while degrading the channel bandwidth.

Channel capacity reduction is raised as a one of the most effective solutions in mitigation of covert channel threats, as full elimination is impossible. The key to success in capacity reduction is the ability to estimate covert channel capacity. However, only a little research has been conducted on covert channel estimation and analysis. Therefore, future research should pay more attention to this area.

With the evolution of network protocols technology and communication technology, it is difficult to maintain security polices or deterrence systems that could limit the rapid growth of network covert techniques. Especially as this is the world of the Internet of Things (IoT), which is motivated by highly effective artificial intelligence tools. Security professional are facing a real challenge.

Future research could focus on developing a security framework that takes into consideration all or most of the aforementioned observations in order to come up with a sufficient security solution to enhance covert channel detectability and enhance prevention tools.

References

ISBN: 978-1-63248-099-6 doi: 10.15224/ 978-1-63248-099-6-71

[1] Q. Yuwen, S. Huaju, S. Chao, W. Xi, and L. Linjie, "Network covert channel detection with cluster based on hierarchy and density," Procedia Engineering, vol. 29, pp. 4175-4180, 2012.

[2] S. Hammouda, L. Maalej, and Z. Trabelsi, "Towards Optimized TCP/IP Covert Channels Detection, IDS and Firewall Integration," in 2008 New Technologies, Mobility and Security, 2008, pp. 1-5.

[3] B. W. Lampson, "A note on the confinement problem," Communications of the ACM, vol. 16, pp. 613-615, 1973.

[4] C. H. Rowland, "Covert channels in the TCP/IP protocol suite," First Monday, vol. 2, 1997.

[5] D. M. Dakhane and P. R. Deshmukh, "Active warden for TCP sequence number base covert channel," in Pervasive Computing (ICPC), 2015 International Conference on, 2015, pp. 1-5.

[6] S. Wendzel, S. Zander, B. Fechner, and C. Herdin, "Pattern-based survey and categorization of network covert channel techniques," ACM Computing Surveys (CSUR), vol. 47, p. 50, 2015.

[7] D. V. Forte, C. Maruti, M. R. Vetturi, and M. Zambelli, "SecSyslog: An approach to secure logging based on covert channels," in Systematic Approaches to Digital Forensic Engineering, 2005. First International Workshop on, 2005, pp. 248-263.

[8] Y. Qian, H. Song, F. Wang, and Z. Wang, "Network Covert Channel Encoding by Packet Length: Design and Detection," Journal of Computational Information Systems, vol. 7, pp. 1463-1471, 2011.

[9] [9] D. Dhobale, V. Ghorpade, B. Patil, and S. B. Patil, "Steganography by hiding data in TCP/IP headers," in Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on, 2010, pp. V4-61-V4-65.

[10] L. Spitzner, "Know Your Enemy: Sebek2 A kernel based data capture tool," ed, 2003.

[11] R. DeGraaf, J. Aycock, and M. Jacobson Jr, "Improved port knocking with strong authentication," in Computer Security Applications Conference, 21st Annual, 2005, pp. 10 pp.-462.

[12] W. Mazurczyk and Z. Kotulski, "New security and control protocol for VoIP based on steganography and digital watermarking," arXiv preprint cs/0602042, 2006.

[13] H. Qu, Q. Cheng, and E. Yaprak, "Using Covert Channel to Resist DoS attacks in WLAN," in ICWN, 2005, pp. 38-44.

[14] S. Craver, "On public-key steganography in the presence of an active warden," in Information Hiding, 1998, pp. 355-368.

[15] S. Zander, G. Armitage, and P. Branch, "A survey of covert channels and countermeasures in computer network protocols," Communications Surveys & Tutorials, IEEE, vol. 9, pp. 44-57, 2007.

[16] A. Epishkina and K. Kogos, "A random traffic padding to limit packet size covert channels," in Computer Science and Information Systems (FedCSIS), 2015 Federated Conference on, 2015, pp. 1107-1111.

[17] L. Barroso and M. Santos, "A Review on Covert Techniques."

[18] G. J. Simmons, "The prisoners' problem and the subliminal channel," in Advances in Cryptology, 1984, pp. 51-67.

[19] T. G. Handel and M. T. Sandford II, "Hiding data in the OSI network model," in Information Hiding, 1996, pp. 23-38.

[20] D. J. Dye, "Bandwidth and detection of packet length covert channels," Monterey, California. Naval Postgraduate School, 2011.

[21] E. Zander, G. Armitage, and P. Branch, "Covert channels and countermeasures in computer network protocols [reprinted from ieee communications surveys and tutorials]," Communications Magazine, IEEE, vol. 45, pp. 136-142, 2007.

[22] J. Zhai, G. Liu, and Y. Dai, "Detection of TCP covert channel based on Markov model," Telecommunication Systems, vol. 54, pp. 333-343, 2013.

[23] P. A. Gilbert and P. Bhattacharya, "An approach towards anomaly based detection and profiling covert TCP/IP channels," in Information, Communications and Signal Processing, 2009. ICICS 2009. 7th International Conference on, 2009, pp. 1-5.

[24] P. Dong, H. Qian, Z. Lu, and S. Lan, "A Network Covert Channel Based on Packet Classification," IJ Network Security, vol. 14, pp. 109-116, 2012.

[25] N. Schear, C. Kintana, Q. Zhang, and A. Vahdat, "Glavlit: Preventing exfiltration at wire speed," IRVINE IS BURNING, p. 133, 2006.

[26] H. Zhao and Y. Q. Shi, "A phase-space reconstruction approach to detect covert channels in TCP/IP protocols," in Information Forensics and Security (WIFS), 2010 IEEE International Workshop on, 2010, pp. 1-6.

[27] [27] T. Sohn, J. Seo, and J. Moon, "A study on the covert channel detection of TCP/IP header using support vector machine," in ICICS, 2003, pp. 313-324.

[28] E. Tumoian and M. Anikeev, "Network based detection of passive covert channels in TCP/IP," in Local Computer Networks, 2005. 30th Anniversary. The IEEE Conference on, 2005, pp. 802-809.

[29] S. J. Murdoch and S. Lewis, "Embedding covert channels into TCP/IP," in Information hiding, 2005, pp. 247-261.

[30] M. Hussain and M. Hussain, "A high bandwidth covert channel in network protocol," in Information and Communication Technologies (ICICT), 2011 International Conference on, 2011, pp. 1-6.

[31] N. D. Rohankar, A. Deorankar, and D. P. Chatur, "A Review of Literature on Design and Detection of Network Covert Channel," International Journal of Engineering Science and Innovative Technology (IJESIT) Volume, vol. 1, 2012.

[32] G. Fisk, M. Fisk, C. Papadopoulos, and J. Neil, "Eliminating steganography in Internet traffic with active wardens," in Information Hiding, 2002, pp. 18-35.

[33] A. Kundu, "Mitigation of Storage Covert Channels in IPSec for QoS Aware Applications," Procedia Computer Science, vol. 54, pp. 102-107, 2015.

[34] M. McFail, "Covert storage channels: A brief overview," in PACISE Conference, Bloomsburg, PA, 2005.

[35] S. Zander, G. Armitage, and P. Branch, "Covert channels in the IP time to live field," in Proceedings of Australian Telecommunication Networks and Applications Conference (ATNAC), 2006.

[36] K. Ahsan and D. Kundur, "Practical data hiding in TCP/IP," in Proc. Workshop on Multimedia Security at ACM Multimedia, 2002.

[37] D. C. Latham, "Department of defense trusted computer system evaluation criteria," Department of Defense, 1986.

[38] Y. A. H. Fadlalla, Approaches to resolving covert storage channels in multilevel secure systems: The University of New Brunswick (Canada), 1997.

[39] Q.-z. YAO and P. ZHANG, "Coverting channel based on packet length," Computer engineering, vol. 34, pp. 183-185, 2008.

[40] L. Zhang, G. Liu, and Y. Dai, "Network packet length covert channel based on empirical distribution function," Journal of Networks, vol. 9, pp. 1440-1446, 2014.

[41] L. Ji, W. Jiang, B. Dai, and X. Niu, "A novel covert channel based on length of messages," in 2009 International Symposium on Information Engineering and Electronic Commerce, 2009, pp. 551-554.

[42] L. Ji, H. Liang, Y. Song, and X. Niu, "A normal-traffic network covert channel," in Computational Intelligence and Security, 2009. CIS'09. International Conference on, 2009, pp. 499-503.

[43] A. S. Nair, A. Sur, and S. Nandi, "Detection of Packet Length Based Network Steganography," in 2010 International Conference on Multimedia Information Networking and Security, 2010, pp. 574-578.

[44] P. Magazine, "7 (51) September 01, 1997, article 06 of 17 [LOKI2 (the implementation)]," ed.

[45] S. Wendzel and J. Keller, "Design and implementation of an active warden addressing protocol switching covert channels," in Proc. 7th International Conference on Internet Monitoring and Protection (ICIMP 2012), Stuttgart, 2012.

[46] S. Wendzel and J. Keller, "Preventing protocol switching covert channels," International Journal on Advances in Security, vol. 5, 2012.

[47] S. Wendzel and J. Keller, "Hidden and under control," annals of telecommunications-annales des télécommunications, vol. 69, pp. 417-430, 2014.

[48] J. Kaur, S. Wendzel, and M. Meier, "Countermeasures for Covert Channel-Internal Control Protocols," in Availability, Reliability and Security (ARES), 2015 10th International Conference on, 2015, pp. 422-428.

[49] R. Rios, J. A. Onieva, and J. Lopez, "Covert communications through network configuration messages," Computers & Security, vol. 39, pp. 34-46, 2013.

[50] L. Garcia, H. Senyondo, S. McLaughlin, and S. Zonouz, "Covert channel communication through physical interdependencies in cyber-physical infrastructures," in Smart Grid Communications (SmartGridComm), 2014 IEEE International Conference on, 2014, pp. 952-957.