A survey of covert channels: Benign and malicious usage, conditions for creation and countermeasures

Ema Stamenkovska
Faculty of Computer Science and Engineering
Ss. Cyril and Methodius University, Skopje
e.stamenkovska92@gmail.com

Vesna Dimitrova
Faculty of Computer Science and Engineering
Ss. Cyril and Methodius University, Skopje
vesna.dimitrova@finki.ukim.mk

***Abstract* - Secure communication is of great importance to everyone, but how to secure a communication when a method that can hide its very existence exists? This can be achieved by a covert channel which can be used for a secret transfer of information. The following article gives a survey of the types of covert channels, the basic conditions for creating an undetectable covert channel as well as the countermeasures that can be taken for its limitation or elimination. An example of a covert channel attack (more specifically DNS tunneling) will be shown. The need for a data leak prevention system, a tool that helps safeguard the sensitive data will be punctuated. Some of the covert channels' uses for corrupt causes will be mentioned. In some cases, security can be actually improved by the use of covert channels.**

***Key words* - covert channel, DNS attacks, DNS benchmark, data loss prevention**

I. INTRODUCTION

Network information hiding is a discipline that deals with the concealment of network communications or their characteristics by encapsulating the capabilities that a particular module has behind an abstract interface. The secret communication channel created by the data hiding method is referred to as a network covert channel and such channels exist throughout the network protocol architecture. It is very important that network designers and security managers understand that while a serious threat even for single hosts exists, the potential for covert channels in computer networks is greatly increased. In computer networks, overt channels, such as network protocols, may be used as carriers for covert channels and their network systems may be effectively subverted in a wide variety of locations within the network [1,2,3,4]. Information hiding can be used for benign purposes, like network authentication, copyright protection etc. but the malicious ones are unfortunately more frequent. Some of them will be described in this survey.

Section II contains information about the classification of covert channels. In section III the basic conditions for creating an undetectable covert channel and the countermeasures that can be taken against covert channels will be viewed more closely. In section IV the main tool that helps safeguard the sensitive data, the data loss prevention system is explained. Section V shows the vast usage of covert channel: for copyright protection, authentication and authorization, for corrupt causes etc. In section VI an example of DNS tunneling is described.

II. CLASSIFICATION OF COVERT CHANNELS

Mainly, there are two types of network covert channels that can be created [5]:

- Covert storage channel, where a process writes data to a storage location, such as hard drive, after which another process of lower clearance is able to read it. So, person A at a low security level is able to read data written by person B at a higher security level. Establishing this type of covert channel is achieved by manipulating the header fields of packets in protocols, like: TCP, IP, ICMP and HTTP. In IP communication that includes changing mostly the ID, source IP address and/or the option field. The option field is used less than the others because it usually gets removed by routers and firewalls [6]. In the transport layer the TCP Initial Sequence Number and the Acknowledgement (ACK) field are used a lot and in the application layer the Domain name system (DNS) ID field is an example of a field exploited for establishing a covert channel [7].
- Covert timing channel, where a process relays information to another by modulating its use of system's resources based on different timing. They actually convey information through arrival timing of packets, and that method is more secure than the storage one, but because of their unpredictable nature (jitter, packet loss and packet reordering events predominant in the Internet) it is possible that they will not be decoded accurately. Some network timing channels require synchronization between the encoder and decoder. Also, these channels are disturbing the traffic patterns and inter-packet intervals of the IP packets. Higher layered protocols may be bothered by this, so by

analyzing those inconsistencies, the timing channel could be detected at a higher layer [8].

III. Conditions for creating a covert channel and countermeasures against its existence

This chapter is divided into two sections, in which firstly are mentioned the basic conditions for creating an undetectable covert channel. Then, some countermeasures that can be taken against covert channels will be shown and explained.

A. Basic conditions for creating an undetectable covert channel

When referring to network information hiding, the warden is the network entity that wants to reveal the existence of the covert channel and later eliminate it [1].

If person A wants to transmit information to person B via a covert channel, the following two conditions needed for achieving covert communication must be met:

- The detecting ability of the warden is practically equal to random guessing
- The probability that B will make a mistake when recovering A's message is close to 0 [9]

Of course, in networking, covert channels are not restricted to unicast (one-to-one) channels. This means A could also send messages to B, C, D and E simultaneously if the channel allows multicast (one-to-many) communication [4].

B. Countermeasures that can be taken against covert channels

The stage of designing a system is crucial, because it can be exploited by the two causes of covert channels:

- Design oversights, that may be repaired if discovered early
- Weaknesses inherent in the system design, that can not be repaired without a system redesign [4]

The possible countermeasures that the warden can take when a covert channel is detected are the following:

- Remove the covert channel [4]

Blocking a connection is the best protection, but it can be implemented only partially by blocking unneeded traffic [7].

- Limiting the bandwidth, which works if the capacity of the channel can be closely estimated [4]
- Auditing the channel by a warden [4]

The shared resource matrix methodology is often used, where all shared resources that can be modified by someone are enumerated and then each one of them is examined whether it can be used to transfer information covertly [10]. Auditing is more useful if the audit event is rare.

- Monitoring and documenting the covert channel, even if it has insignificant capacity [4]

Proxies can be used as a second layer of protection between an enterprise and the Internet. Incoming and outgoing connections finish at the proxy and the proxy server hides the user's IP address. All the hidden information stored in the lower layers is going to be lost. Most of the proxies also work in the application layer and check for abnormalities. They can filter the content, looking for known patterns [7].

The job of taking countermeasures should be entrusted to the best warden. There is a distinction between a passive warden, who can only spy on the channel, and an active warden who is able to modify the messages, but their context must remain the same [4]. This is a generalization because there are many subtypes of wardens. The best warden is a dynamic adaptive warden that with as fewer rules and effort as possible is adaptively limiting the capabilities of those who are using the covert channel and makes it difficult for them to deduce warden's strategy [1].

IV. Solution for data loss prevention

All modern enterprises and organizations in every industry have data and depend on data sharing. For preventing a data breach to occur, a data leak (or loss) prevention system is needed. That is a tool that helps safeguard the sensitive data. In case a violation occurs, the data loss prevention (DLP) solution must provide historic information for forensic analysis. There are different types of DLPs needed for achieving a secure work space in a multi-organization environment [11].

End-point based DLP includes data-in-use, because this data is "used" by the enterprise's employees on end-point devices. The DLP applies end-point security methods, so that data can travel safely in the case when there is no Internet connection. Sometimes employees use USBs for storing and passing company data. A USB memory device is developed that can erase the data if the USB is lost and the sensitive data can be passed only to the allowed servers and PCs [11].

Network based DLP takes care of data leaving the enterprise via a network. It includes the data-in-motion. A great concern is monitoring and controlling outbound Internet communication, where data can be lost through many channels, such as web mail and FTP transfer. [12].

Data-at-rest, static data stored on enterprise devices also should be protected by the DLP system. Most enterprises should apply control access rights to sensitive data not only located outside, but also inside the company. The security technology that achieves that is called Enterprise Rights Management (ERM) [11]. It manages usage

restrictions (printing, editing, viewing etc.). This can be accomplished with a server. [11, 13].

After discovering the three types of company data, the DLP solution should identify the sensitive data and enforce policies to that data. The existing DLP systems rely on hashing, keywords, regular expressions, fingerprinting etc., so they actually rely on humans. They can not completely recognize and classify the sensitive information by themselves. There is a need for this classification to be automated by efficient machine learning algorithms [13].

Even if the DLP systems manage to successfully face the challenges of performance and accuracy [13], as cloud computing becomes used more often, a problem arrives, where a company and the customers have to have trust in the cloud provider, because they share and confide the management of their information to a third party [11]. A combination of Public Key Infrastructure (PKI), Lightweight Directory Access Protocol (LDAP) and Single sign-on (SSO) can address most of the concerns about integrity, authenticity, confidentiality and availability of data and communications [14]. The cloud providers are having themselves audited by certification systems, because they realize that it is essential that they gain the companies' and the customers' trust [11, 14].

V. USAGE OF COVERT CHANNEL

This chapter is divided into two sections, in which examples of different uses of covert channel, both benign and corrupt will be mentioned and explained.

A. Usage of covert channel for copyright protection, authentication and authorization

The data hiding method can be used for copyright protection, authentication and authorization. This could be achieved by diverse applications such as copyright protection for digital media, watermarking, fingerprinting and steganography. The communication patterns could be detected if we use only encryption. So there is a need for technologies that can protect content even after it is decrypted [15, 16]. Such technologies are the following:

- In watermarking applications, the message contains information (such as owner ID and a digital time stamp) placed within the content where it is never removed during normal usage [15, 16].
- The fingerprint sensor reads the ridge pattern on the finger surface and converts the analogue reading in a serial number that uniquely identifies the owner [17]
- Steganography is covert channel's oldest form (in a way, covert channels equals network steganography) [7]. The main difference between steganographic and cryptographic methods is that the first ones hide information by making it difficult to notice, and the cryptographic ones do that by making it difficult for recognition [2]. Steganography hides a secret message within the host data set which does not noticeably change the data. A simple example for this is changing the least significant bits to embed information in an image file. Its presence can not be detected (the picture will look the same) when nobody suspects transmission of a hidden data [6, 15].
- Port-knocking allows authorised users to access open firewall ports and to all other users these ports appear to be closed [4]

B. Usage of covert channel for corrupt causes

The covert channels can be used for illicit manner, like changing and leakage of confidential data. Almost every protocol can be used as a covert channel by carrying another protocol with a technique called tunneling. Hackers use the hidden network to escape from firewalls and IDSs (intrusion detection systems). There are many examples of uses of covert channels for corrupt causes.

Computer viruses and worms can use covert channels to self-replicate and spread copies of themselves undetected and/or exchange information for distributed processing, like brute-force attacks [4]. Most Trojans and botnets use covert channel communication, mostly over HTTP [7]. Trojans may send an instruction to a server on a compromised system through a covert channel. If the IDS consider it to be ordinary, the Trojans can communicate to the hacker (the client component) and not be detected. "Bots" is derived from "robot", because it is a malware that can act similar to a human being, and can launch DoS attacks and use covert channels to gather passwords, confidential information, log keystrokes, analyze traffic etc [18]. It is interesting that for DoS attacks, a packet traceback technique that uses covert channels for filtering the attack traffic and isolating the attacker is developed [4].

It was mentioned that covert channels can be used for authentication, but they can also break anonymity. There is a covert-channel based technique that can identify locations of sensors with probe response attacks [4].

VI. AN EXAMPLE OF A COVERT CHANNEL ATTACK THAT EXPLOITS DNS TUNNELING

The Domain Name System (DNS) is a network service that translates host names into numerical IP addresses. For almost any network, a communication with a DNS server is needed.

Unfortunately, one of the most often used backdoor by hackers is the DNS. This is due to its wide availability and the fact that usually it is not monitored by common security measures, like firewalls, proxies and IDS because it is not intended for transfer of data [19]. IDC reports that 82% of companies worldwide have faced a DNS attack over the past year, which is based on a survey IDC conducted on behalf of DNS security vendor EfficientIP of 904 organizations across the world during the first half of 2019. The average costs associated with a DNS attack rose

by 49% compared to 2018 and most companies resolved the DNS attack after more than a few days [20]. In a research conducted by Palo Alto Networks Unit 42 in 2019 was found that up to 80% of malware uses DNS to establish command and control [21].

Hackers may achieve this attack successfully by establishing a covert communication channel. The channel is set between the device inside the network running a tunneling technique like Iodine, NSTX, DNSCat2 etc. and a server on the Internet and then they communicate back and forward through the DNS tunnel to control the compromised device.

There is a second more malicious approach done by dropping a malware. The malware encrypts a file usually containing sensitive information, dissects it and sends it in a form of multiple DNS queries to a server controlled by the attacker. This approach is shown at Figure 1 [22].

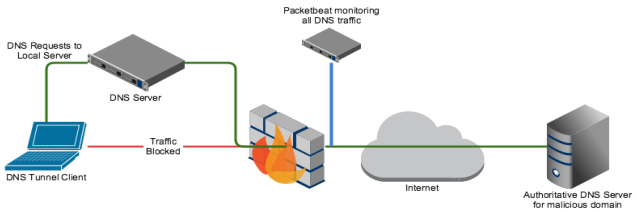

Figure 1. DNS approach done by dropping a malware

A common example of deploying robust secret communication is done by a simple steganography scheme through spam e-mails. This scheme can offer unidirectional asynchronous one-to-one or one-to-many covert channel facilities that are able to bypass firewalls and traffic analyzers [23]. DNS cache poisoning is often found in URLs sent via spam emails. By exploiting system vulnerabilities, attackers can inject malicious data into your DNS resolvers' cache. This is an attack technique often used to redirect victims to another remote server [22].

As a response toward the great DNS tunneling concern, researchers are tending to use Machine Learning Techniques (MLTs) to detect tunneling. These detection techniques can be grouped into two categories: payload analysis and traffic analysis [19]. Infoblox, for example, is a patented technology that uses machine learning and can even show exactly which devices or employees are trying to steal data [24].

It is also useful to notice that there are many free DNS projects that offer different Internet experience. The one that Google offers is the most known (with ip address 8.8.8.8). The newest DNS projects are made by: CleanBrowsing (185.228.168.9), Quad9 (9.9.9.9) and Cloudflare (1.1.1.1) [25].

We added the four addresses mentioned above to DNS Benchmark freeware, we ran the benchmark on the laptop and we got the results that can be seen at Figure 2 and Figure 3.

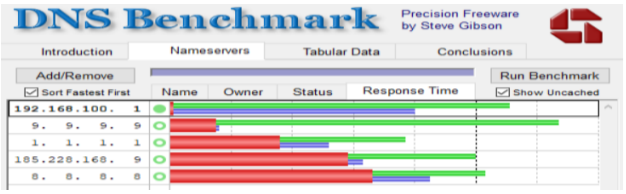

Figure 2. DNS Benchmark results 1

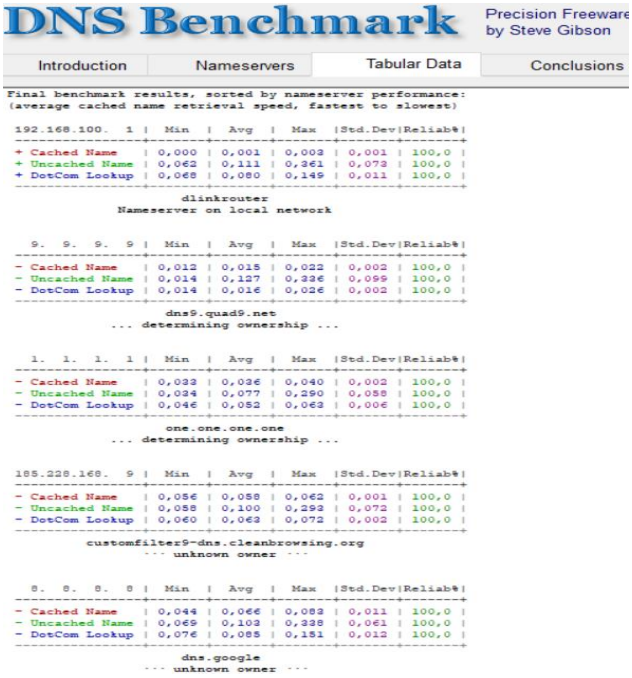

Figure 3. DNS Benchmark results 2

The first address is from the router and it has the best results related to latency. The Google's server had the worst results compared to the "new DNS players". CleanBrowsing is mostly used for content filtering and offers browsing the Internet without unwanted surprises [26]. Quad9 uses response policy zones to prevent tunnelling and phishing sites. When a user tries to go to such site, he encounters a walled garden and is warned of risky behaviour [21]. Information about personal id is not collected by the system [27]. Cloudflare is audited by KPMG to ensure that the customers' IP address and what they do is not kept by them. They delete the logs within 24 hours of their appearance. DNS has been largely unencrypted since its creation. Lately, there has been a push for using techniques for encrypting DNS over TLS and over HTTPS. Now, on the server side, Google DNS and Cloudflare's DNS support them. These techniques can increase latency, but it can be amortized over many queries. Chrome will probably adopt Google DNS and Firefox – Cloudflare, which could mean centralization of encrypted private information to them instead of unencrypted private information to many ISPs.

VII. Conclusion

Network covert channels can be used by attackers to help them steal information from compromised hosts. The DNS tunneling attack that was mentioned as an example is

simple to execute, and still can cause serious problems. It is a great challenge to maximize data leak protection system's performance and accuracy. On the other hand, the covert channels can also be used for delivering privacy information, like passwords, social security numbers, trade secrets etc. more securely [5, 11].

For some applications, the warden is an antagonist (for e.g. a censor in an oppressive regime). For others, it is trying to prevent the actions of an antagonist (for e.g. a malware) [1].

It is crucial for more to be done about better regulation.

REFERENCES

[1] W. Mazurczyk, S. Wendzel, M. Chourib, J. Keller, "Countering adaptive network covert communication with dynamic wardens", Future Generation Computer Systems Volume 94, May 2019, pp. 712-725

[2] W. Mazurczyk, S. Wendzel, S. Zander, A. Houmansadr, K. Szczypiorski, "Information hiding in communication networks: fundamentals, mechanisms, applications, and countermeasures", Wiley Online Library, 2016

[3] T. G. Handel, M. T. Sandford II, "Hiding Data in the OSI Network Model", International Workshop on Information Hiding IH 1996: Information Hiding, pp. 23-38

[4] S. Zander, G, Armitage, P. Branch, "A survey of covert channels and countermeasures in computer network protocols", IEEE Communications Surveys & Tutorials, July 2007

[5] Y. Qian1, T. Sun, J. Li, C. Fan, H. Song, "Design and analysis of the covert channel implemented by behaviors of network users", 2012 Sep, 31(9): 1611-24. DOI: 10.1007/s00299-012-1275-3. Epub 2012 May 20.

[6] S. Z. Gober, B. Javed, N. A. Saqib, "Covert Channel Detection: A Survey Based Analysis", 9th International Conference on High Capacity Optical Networks and Enabling Technologies HONET 2012, DOI: 10.1109/HONET.2012.6421435

[7] J. Selvi, "Covert Channels Over Social Networks", 2019

[8] X. Luo, E. W. W. Chan, R. K. C. Chang, "TCP Covert Timing Channels: Design and Detection", Conference Paper, July 2008, DOI: 10.1109/DSN.2008.4630112 ·

[9] J. Wang, W. Tang, Q. Zhu, X. Li, H. Rao, S. Li, "Covert Communication with the Help of Relay and Channel Uncertainty", 2018

[10] R. A. Kemmerer, "Shared Resource Matrix Methodology: An Approach to Identifying Storage and Timing Channels", ACM Transactions on Computer Systems, Vol. 1, No. 3, August 1983, pp. 256-277

[11] T. Takebayashi, H. Tsuda, T. Hasebe, R. Masuoka, "Data Loss Prevention Technologies", FUJITSU Sci. Tech. J., Vol. 46, No. 1, pp. 47–55, 2010

[12]https://www.cisco.com/c/en/us/products/collateral/security/web-security-appliance/solution-overview-c22-738537.html

[13] M. Hart, P. Manadhata, R. Johnson, "Text Classification for Data Loss Prevention", 2011

[14] D. Zissis, D. Lekkas, "Addressing cloud computing security issues", Future Generation Computer Systems Volume 28, Issue 3, March 2012, Pages 583-592

[15] M. M Amin, M. Salleh, S. Ibrahim, M.R.K Atmin, M.Z.I. Shamsuddin, "Information Hiding using Steganography", February 2003, DOI: 10.1109/NCTT.2003.1188294

[16] I. J. Cox, M. L. Miller, T. Kalker, "Digital Watermarking and Steganography" Elsevier, 2007

[17] D. Maltoni, "Handbook of Fingerprint Recognition", Springer, 2009

[18]https://tools.cisco.com/security/center/resources/virus_differences

[19] S. Yassine, J. Khalife, M. Chamoun, H. el Ghor, "A Survey of DNS Tunnelling Detection Techniques Using Machine Learning", Published in BDCSIntell 2018

[20]https://www.networkworld.com/article/3409719/worst-dns-attacks-and-how-to-mitigate-them.html

[21] T. Olzak, "DNS Tunnelling Identification and Defence", 2019

[22]https://securitytrails.com/blog/most-popular-types-dns-attacks

[23] A. Castiglione, A. De Santis, U. Fiore, F. Palmieri, "An asynchronous covert channel using spam", Computers & Mathematics with Applications, Volume 63, Issue 2, January 2012, pp. 437-447

[24]https://www.infoblox.com/solutions/service-providers/secure-dns-caching/

[25]https://medium.com/@nykolas.z/dns-resolvers-performance-compared-cloudflare-x-google-x-quad9-x-opendns-149e803734e5

[26]https://cleanbrowsing.org/

[27]https://quad9.net/about/