Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 03, March -2018

COVERT CHANNEL AND COUNTERMEASURES IN THE OSI NETWORK MODEL

Dr Dhananjay M. Dakhane[1], Jaya Harishrao Tayde[2]

[1]Computer Science, Sipna C.O.E.T. Amravati
[2]Computer Science, Sipna C.O.E.T. Amravati

Abstract — *Covert channels are used for the secret transfer of information. Now a day's covert channel it is an interesting study area. A Covert channel can be used to pass a wicked message. The message can be any form such as computer virus, spy programs, terrorist messages etc. A Covert channel is defined as it is a way of abstracting the information and hiding the information, in such a way that the person who reads should not examine the hidden information and transmits the data to the destination. A covert channel uses the different field to hide the data. In this paper, we use the different network protocol of OSI model. This paper presents the basis for the development of a toolkit for creating and exploiting hidden channels within the standard design of network communication protocols. The data can be wicked software or virus that can be communicated through the unauthorized channel. This paper focuses on the methods of hiding and countermeasures.*

Keywords- *covert channel, IEEE 802.11, OSI model, wicked message.*

I. INTRODUCTION

Frequently it is thought that the use of encryption is sufficient to secure communication. But encryption only prevents unauthorized parties from decoding the communication. Many innovations in the field of cryptography contain made in current decades, ensuring the privacy of the message's content. However, sometimes it is not enough to secure the message and communicating parties need to conceal the fact of the being of any communication. The need to protect secret messages appeared for a long time. This problem is solved by covert channels.

A covert channel is similar techniques for hiding information as like steganography. In steganography we can hide the data in the form of visual or text content, there is requires some form of content as a wrap and in covert channels, there is required a few network protocols as a carrier. Network covert channels, are concealed and potentially policy breaking communication channels initially introduced as unpredicted communication channels by Lampson [1]. Lampson introduced covert channels in 1973 in the framework of massive systems as a mechanism by which a process at a high-security level leaks information to a process at a low- security level that would or else not have access to it [2]. In computer networks, the capability of covert channels has more increases rapidly due to high- speed network technologies. Because we could lose 26GB of data annually at internet site if we send only one bit per packet secretly [3]. The purpose of using network covert channels is to transfer information over the network as ensuring that the transfer is not known by a third party. Whenever system builders intend secure systems, they build these systems starting with a set of assumptions – one common way is that to break security systems is via violating these assumptions. This principle is illustrated clearly by covert channel attacks where two entities can communicate by manipulating shared resources in not deliberate ways; In a Covert channel, there are usually three communication steps. Primarily a first step is to send mechanism. In send mechanism, we send bits of data by manipulating a shared resource. The second mechanism is a receiving mechanism in which a different process infers the bits by monitoring a shared resource. At last is optional feedback mechanism back to the sender provides direct synchronization and reduces noise. In preceding work, the receive and feedback mechanisms for a given attack, use the same communication mechanism.

A Covert channel has much application are of a wicked or avoidable nature and therefore pose a serious threat to network security. In addition, we think that because of improved measures against open channels, such as the free transfer of memory sticks in and out of organizations as described in computer network use of covert channel will increase. Considerate existing covert channel techniques are essential in developing countermeasures.

A covert channel it is a technique of hiding the data in such way that no one can be identified so due to that there is a difficulty of detection, elimination and capacity limitation but it has to require to be addressed to safe future computer networks. In this paper, there is a study of countermeasure for covert channels in network and application protocol. A further connected area is the field of indistinct communications concerned with obfuscating sender/recipient identities and their relationships (who is communicating with whom) [4]. But this topic does not address full secrecy of communication, as observers can still end that some form of communication is taking place [5].

II. COVERT CHANNEL

A Covert channel is a way of abstracting the information and hiding the information, in such a way that the reader should not analyze the hidden information and send the facts to the destination. In this section, we give an overview of existing covert channel techniques in computer network protocols of OSI model. In this paper, we described a different typical hidden channel which is design for layers of Open system interconnection.

2.1. Hiding Data in the Application Layer

2.1.1 Function of the Application Layer: The application layer is nearest the user. Users create applications utilizing system resources, including the network. Functional examples include browsers (Mosaic), terminal emulators (telnet), file transfer programs (FTP), email, word processing, and distributed databases.

2.1.2 Language Manipulation: Many of the classical steganography approaches can be used at the application level. What was originally done with pencil and paper can be done here.

2.1.3. Hypertext Transfer Protocol (HTTP): In modern years, web applications, such as web browsers, email clients, and web messengers have become necessary elements in business and everyday life. That's why everywhere HTTP messages are so useful for covert information containers. In the implementation of covert channels, the use of HTTP may increase the capacity of the covert channel because of HTTP's flexibility and large division as well. We propose a detailed analysis HTTP covert channels and techniques of their detection and capacity limitation. The information is hidden in JavaScript/HTML and transported through the use of JavaScript redirects. A viewer who cannot look into the content transported by HTTP [6] cannot distinguish between harmless web surfers and the covert senders/receivers. Feamster *et al.* proposed Infranet — a framework to use covert channels in HTTP to avoid restriction.

2.2 Hiding Data in the Presentation Layer

2.2.1 Function of The Presentation Layer: The presentation layer handles the network's interface to devices, such as printers, video displays, and the file system. The presentation layer is what begins to make differences in operating systems transparent. The presentation layer is the proper place for encryption and compression processes, etc.

2.2.2 Data Embedding: The multimedia components of the presentation layer can act as hidden data transport mechanisms. The statistical properties of audio and video information contain stochastic noise that can be characterized and modified. The stochastic noise can be replaced with pseudo-random noise containing hidden data. Multimedia files are traditionally large data sets, making them attractive hosts for storing hidden data. Much of the presentation layer facilitates transporting data in the system. Data can be hidden within the fields of system messages that are passed to all active processes.

2.3. Hiding Data in the Session Layer

2.3.1. The Function of the Session Layer: The session layer is the user's access point to the network. The session layer establishes connections between processes on different hosts, thus the name "session." Users retain full control over their workstation, but accessing the network requires user ID and password. Once on the network, users may have access to restricted resources of other users on the network, including servers that may require further authentication. Functionality at the session layer is achieved by a redirector.

2.3.2. Covert Channel Using Session Level Redirectors: The most common use of a redirector is to "mount" remote disks on a local machine. If a user can read a remote disk, then a covert channel can be established. For example, Bob may place two files on his disk that Alice can read remotely. Bob can check his local disk activity. Whenever Alice reads the first file, Bob records a logical zero, and when she reads the second file, Bob records a logical one. The file contents are irrelevant. Thus, Walter's suspicions are not raised.

2.4. Hiding Data in the Transport Layer

2.4.1. The Function of the Transport Layer: The main function of the transport layer is responsible for delivering data from the network to within the host computer. The transport layer must interact with multiple programs running on the host and has system level access to processes. Transmission Control Protocol (TCP) is the Internet implementation of this layer.

2.4.2. TCP Packet Manipulation: There are unused data bits in the TCP header similar to those found in the IP header. Six bits are available between the data offset byte and the urgent pointer. These bits are not used in the current implementation. These six bits, combined with the two bits in the IP header give one byte of hidden data per packet transmitted. Walter can discover the use of this reserved space if he has packet monitoring in place to detect the usage of reserved areas.

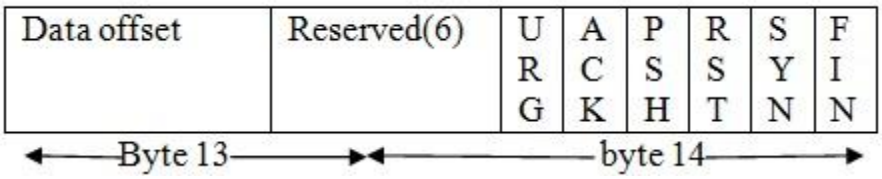

Figure 1: Reserved Bytes in TCP Packet Header

2.5. Hiding Data in the Network Layer

2.5.1. The Function of the Network Layer: The network layer is the internal delivery system. Routing information and error control are added to the data as headers and trailers that define the source and destination for the packet. This layer assures correct delivery and receipt of packets. The network layer may fragment packets at the source and reassemble them at the destination or at an intermediate location.

2.5.2. Hiding data in the Internet Packet: Within the IP packet header there is an 8- bit type-of-service byte of which the two least significant bits are not used in the current implementation. The bits can be used to store more information. Packets sent on even time increments represent a logical zero. Packets sent in odd increments represent a logical one. Time stamping is normally used for diagnostic testing and accounting Purposes. Destruction of hidden will occur if intermediate handling devices (such as routers) are modified to strip out data from these' locations.

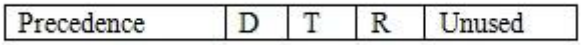

Figure 2. IP Type of Service Field

2.6. Hiding Data in the Data Link Layer

2.6.1. The Function of the Data Link layer: The data link layer shapes the network data structure. Frames are created containing facts to be transmitted over the physical circuits. Frame headers contain to/from information. Trailers contain error control information (usually a cyclic redundancy check -- CRC). The primary function of the data link layer is to prevent data corruption within the physical layer.

2.6.2. Data Frame Manipulation: In data frame manipulation we stored a covert data as unused portions of the frame. Hidden data is stored in the buffer, beginning at the end of the buffer and working toward the valid data. When the packet is transmitted, the buffer is exported, including the covert data. Some minor software changes may be required. It is necessary to reduce the greatest number of legitimate bytes by two in order to provide at least one byte of hidden storage per packet. The second byte of the two is used as a "data separator."

2.6.3. 802.11 MAC frame format: Each frame consists of the following basic components [7]:

a) A MAC header contains duration, addresses, frame control, and sequence control information.

b) A variable length frame body, which has information specific to the frame type.

c) A frame check sequence (FCS), which has an IEEE 32-bit cyclic redundancy code (CRC) format. Frame type contains the address field which is address 2, address 3, sequence control and address 4. In the case of secure network, i.e. if the LAN is configured to support WEP encryption, 802.11 MAC frame has the format presented in where the initial vector (IV) is a random value used to encrypt the payload with RC4 algorithm and the integrity check value (ICV) is computed to check if the payload was altered during transmission.

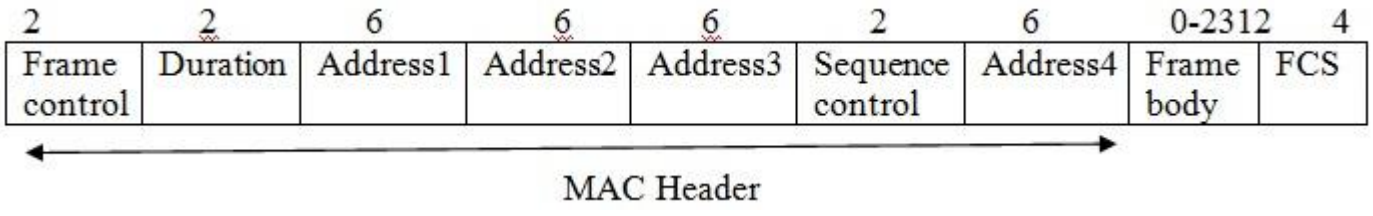

Figure 3.Generic 802.11 MAC frame format

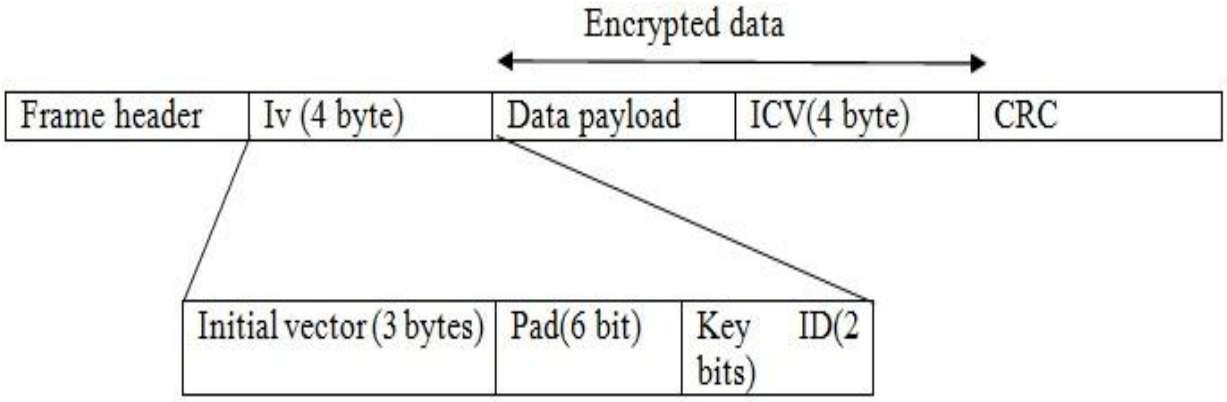

Figure 4. 802.11 MAC Frame Armed With WEP

2.7. Hiding Data in the Physical Layer

2.7.1. The Function of the Physical Layer: The main function of the physical layer is to send a data through communication channels. The physical layer has all hardware which is necessary carry out this task. The major part of this hardware is network interface card. The communication method, including control signals and timing, are included in the physical layer.

2.7.2. Serial Communications Port Manipulation: There is a difference between channel capacity and throughput. The baud rate of the serial communications port can be adjusted over a wide range, and its setting generally defines the channel capacity. The throughput is adjusted by a handshaking mechanism that controls data flow. This mechanism is necessary for the event that data cannot be processed as quickly as it is received. Throughput can be biased using the Clear to Send/Ready to Send (CTS/RTS) signals, and can be adjusted independently from the data rate.

III countermeasures

If a covert channel has been identified the usually obtainable countermeasures are:

• Eliminate the channel

• Limit the bandwidth of the channel

• Audit the channel

3.1. Eliminating Covert Channels

In this, we have a host security to remove a covert channel but host security cannot remove covert channel but it helps to prevent exploitation in some scenarios. For example, on the Internet, some protocols cannot be blocked because they are fundamental (e.g., IP, TCP) or their services are too significant (e.g., HTTP). On the other hand in a closed network protocol prone to covert channels could be blocked-up or replaced with fewer or limited covert channels. The leakage of classified information from a high-security system to a low-security system is prevented by a network design where only hosts on the same security level are allowed to communicate. With the help of normalizing protocol headers, padding, and header extensions we can easily eliminate storage covert channels. For example, reserved bits and padding are located to zero, and indefinite header extensions are removed. Other header fields can be normalized.

3.2. Limiting Covert Channel Capacity

In this section, we described a technique that can be used to limit the capacity of some channel. In limiting covert channel capacity first, we have to estimate a capacity. Once we count the address modulation channel this is the way to limit the number of passable address efficiently limiting the allowed host to host connections. If all packets having padding of the same size then it can easily drop the packet length modulation channel. If a packet is of small it allows increasing efficiency. A number of techniques have been proposed to limit the capacity of covert channels in the timing of acknowledgments.

3.3. Auditing Covert Channels

All proposed detection methods are based on the detection of nonstandard or abnormal behavior. The statement is that the warden knows the normal behavior of protocols and hosts, and can detect anomalous behavior caused by covert channels. However, it is difficult to detect covert channels if there is much variation in normal behavior. In addition, any covert channel that appears the same to the normal use of the protocol will be hard to detect. A protocol which is based on nonstandard and that can be used covert channel can be easy to detect. There are various methods have been proposed to detect packet timing channels. Some researchers have proposed auditing the change of traffic rate over time. If one host changes the traffic rate by more than a positive threshold, this would show a covert channel. Other researchers have planned for detecting these channels based on the packet interracial time-sharing a number of solutions have been proposed for detecting payload tunneling channels.

IV. Conclusion

The paper describes covert channel to hide information in the network protocol of OSI model. We have introduced the idea and communication model of covert channels and explained the different application countermeasures used to detect, drop, or limit the capacity of covert channels. Many existing covert channels in network protocols follow the security Covert channels in upper network layers may be more attractive as they offer larger bandwidth and allow users to exchange covert messages. A There are some directions for further research. At present, a complete organization for classifying the different covert channels and countermeasures is missing. Covert channels by now have been used just to leak sensitive information, such as secret keys and passwords. Recently, however an idea of using covert channels to protect the data. Several directions are left for further study. We must have focused on capacity estimation. Because of capacity estimation include formal methods and channel errors to find covert channels during protocol design.

REFERENCES

[1] B. W. Lampson, "A note on the confinement problem," *Commun. ACM*, vol. 16, no. 10, pp. 613–615, 1973.

[2] B. Lampson, "A Note on the Confinement Problem," *Commun. ACM*, vol. 16, no. 10, Oct. 1973, pp. 613–15.

[3] G. Fisk *et al.*, "Eliminating Steganography in Internet Traffic with Active Wardens," *Proc. 5th Int'l. Wksp. Information Hiding*,Oct. 2002

[4] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The Second generation Onion Router," *Proc. 13th USENIX Security Symp.*, Aug. 2004

[5] G. Danezis, "Covert Communications Despite Traffic Data Retention," tech. rep., ESAT, University of Leuven, Jan. 2005, http://homes.esat.kuleuven.be/~gdanezis/cover.pdf

[6] A. Dyatlov and S. Castro, "Exploitation of Data Streams Authorized by a Network AccessControl System for Arbitrary Data Transfers: Tunneling and Covert Channels over the HTTP Protocol," tech. rep., Gray-World, June 2003, http: / /gray-world.net/projects/papers/covert_paper.txt

[7] LAN MAN Standards of the IEEE Computer Society. IEEE Standard 802.11. Wireless LAN Medium Acess Control MAC and physical layer specification, 1999.

