A Review on Covert Techniques

Luis Barroso
Department of Computer Science
Faculty of Sciences
University of Porto

Marcelo Santos
Department of Computer Science
Faculty of Sciences
University of Porto

***Abstract*—The creation of covert channels in public computer networks can prove an effective means of information hiding and secret communication. With the widespread adoption of the Internet the TCP/IP suite of protocols have become pervasive, and therefore an attractive target for covert channel exploitation. In this paper we will explore some covert techniques and countermeasures.**

I. Introduction

Definir Covert Channel + Overt Channel + introduo ao resto do paper

II. Covert Techniques

In thes section we give an overview of some covert channel techniques. There will be presented only a few examples among all the existing techniques. The selection was based on their usage and exploit frequency.

A. Unused Header Bits

By exploiting protocols, such as TCP/IP, it is possible to encode a covert channels using reserved or uneused bits of their headers, as proven in [2]. If protocol standards do not impose specific values to their headers, or receivers do not check for the standard values, covert data can be transmitted, for example in IP header's type of service field. In figure 1 we can see TCP/IP header and their exploitable fields, marked as underlined.

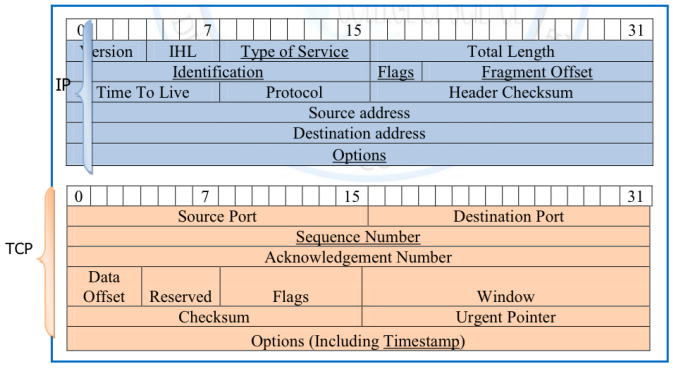

Fig. 1. TCP/IP Header Structure

Another possible exploit regards padding bits. If protocol standard does not enforce specific values for padding, any data can be covert within those padding bits.

B. Optional Header Fields

In spite of the usage of predefined header extensions regarding discretionary information transport on requisition, many protocols still allow header extensions to carry data unpredicted in the original specification in order to augment the proficiency of protocols. One simple example is to covert data masked as IP addresses in IP route record option headers.

C. Semantic Overloading of Header Fields

A different approach regarding covert techniques is the semantic overloading. It consists of exploiting syntactic variations of the overt channel to encode covert data whilst the channel is maintained semantically identical. For example, using TCP sequence numbers in TCP header, it is possible to encode covert data. in order to do it, the client chooses the ISN (Initial Sequence Number), and it should be choosen carefully so that the sequence numbers of new incarnations do not overlap with the ISNs earlier incarnations. Using the most significant byte of each ISN and setting the remaining bytes to zero it is possible to create a covert channel, as proven in [**?**]. In higher layer protocols, mainly text-based ones, like Hypertext Transfer Protocol (HTTP), offer further opportunities. Covert channels can be created by varying the use of upper and lower case, or the number of white spaces between words.

D. Modulating Header Fields

Subsection text here.

E. Packet and Message Sequence Timing

Another technique relies on sequence timing. To establish a covert channel, the sender varies its packet rate each time interval, and the receiver measure packet's rate in each time interval and decodes the hidden information. However, packet timing channels required synchronization mechanisms at both,sender and receiver sides, in order to alter the packet rate and obtain proper readings at the destination.

F. Indirect Channels

Subsection text here.

G. Payload Tunneling

Subsection text here.

H. Hypertext Transfer Protocol (HTTP)

Subsection text here.

I. Wireless LAN (WLAN)

Subsection text here.

III. Applications

covert channels by H.Rowland [2] mencionar papers do skype e tcp/ip?

IV. Countermeasures

texto introdutrio.

A. Eliminating Covert Channels

Subsection text here.

B. Limiting Covert Channel Capacity

Subsection text here.

C. Auditing Covert Channel

Subsection text here.

V. Conclusion

The conclusion goes here. [3] [1]

Acknowledgment

The authors would like to thank...

References

[1] David Llamas, C Allison, and A Miller. Covert channels in internet protocols: A survey. In *6th Annual Postgraduate Symposium about Convergence of Telecommunications, Networking and Broadcasting*, 2005.

[2] Craig H. Rowland. Covert channels in the tcp/ip protocol suite. *First Monday*, 2(5), 1997.

[3] Sebastian Zander, Grenville Armitage, and Philip Branch. A survey of covert channels and countermeasures in computer network protocols. *Communications Surveys & Tutorials, IEEE*, 9(3):44–57, 2007.