Abstract

Covert channels use stealth communications to compromise the security policies of systems. They constitute an important security threat since they can be used to exfiltrate confidential data from networks. TCP/IP protocols are used everyday and are subject to covert channels problems. Covert channels are used for the secret transfer of information. Encryption only protects communication from being decoded by unauthorized parties, whereas covert channels
Aim to hide the very existence of the communication. Initially, covert channels were identified as a security threat on monolithic systems i.e. mainframes. More recently focus has shifted towards covert channels in computer network protocols. The huge amount of data and vast number of different protocols in the Internet seems ideal as a high-bandwidth vehicle for covert communication. The aim of this paper is to give an overview of covert channels in TCP/IP networks. We briefly describe the TCP and IP protocols, present the different types of covert channels and the methods to set them up in TCP/IP networks; then we study the existing methods to detect and eliminate covert channels.

References

- Sebastian Zander and Grenville Armitage, and Philip Branch, SWINBURNE UNIVERSITY OF TECHNOLOGY MELBOURNE, AUSTRALIA "A Survey of Covert channels and countermeasures in computer network protocols", IEEE Communications Surveys & Tutorials 44 • 3rd Quarter 2007
- Pierre Allix, Covert channels analysis in TCP/IP networks, 2007
- "Covert Channel Analysis and Data Hiding in TCP/IP" by Kamran Ahsan
- H. Qu, Q. Cheng, and E. Yaprak, “Using Covert Channel to Resist DoS Attacks in
- “The Implementation of Passive Covert Channels in the Linux Kernel”, Joanna Rutkowska, Chaos Communication Congress December 2004
- “Embedding Covert Channels into TCP/IP” by S.J. Murdoch, S. Lewis, University of Cambridge, United Kingdom, 7th Information Hiding Workshop, June 2005
- Dr. T.R. Sontakke, Sanjeev Wagh, Prashant Yawalkar, “Eliminating covert channels in TCP/IP using active wardens”

Index Terms

Computer Science

Information Technology

Keywords

Keywords— Covert channels  Steganography  TCP  IP  computer security networking
detection

protection

analysis

traffic normalisers
packet sorting