BSDCan 2009 Proposal

Title: **Results of a Security Assessment of the TCP and IP protocols and Common Implementation Strategies**

Estimated duration: 1 hour

Target audience: advanced/expert

Required skills: TCP & IP internals

Speaker: Fernando Gont (fernando@gont.com.ar)

Speaker's Affiliations: Research project carried out on behalf of the United Kingdom's Centre for the Protection of National Infrastructure (CPNI).

Description

Fernando Gont will present the results of security assessment of the TCP and IP protocols carried out on behalf of the United Kingdom's Centre for the Protection of National Infrastructure (Centre for the Protection of National Infrastructure). His presentation will provide an overview of the aforementioned project, and will describe some of the new insights that were gained as a result of this project. Additionally, it will provide an overview of the state of affairs of the different TCP/IP implementations found in BSD operating systems with respect to the aforementioned issues.

Reason why this material is innovative or significant

The TCP/IP protocols were conceived during a time that was quite different from the hostile environment they operate in now. Yet a direct result of their effectiveness and widespread early adoption is that much of today's global economy remains dependent upon them.

While many textbooks and articles have created the myth that the Internet Protocols were designed for warfare environments, the top level goal for the DARPA Internet Program was the sharing of large service machines on the ARPANET. As a result, many protocol specifications focus only on the operational aspects of the protocols they specify and overlook their security implications.Though Internet technology has evolved, the building blocks are basically the same core protocols adopted by the ARPANET more than two decades ago.

During the last twenty years many vulnerabilities have been identified in the TCP/IP stacks of a number of systems. Some were flaws in protocol implementations which affect only a reduced number of systems. Others were flaws in the protocols themselves affecting virtually every existing implementation. Even during the last few years researchers have still been working on security problems in the core protocols.

The discovery of these vulnerabilities led in most cases to reports being published by a number of CSIRTs and vendors, which helped to raise awareness about the threats and the best possible mitigations known at the time the reports were published. However, for some reason much of the effort of the security community on the Internet protocols did not result in official documents (RFCs) being issued by the organization in charge of the standardization of the communication protocols in use by the Internet: the Internet Engineering Task Force (IETF). This basically led to a situation in which "known" security problems have not always been addressed by all vendors. In addition, in many cases vendors have implemented quick "fixes" to the identified vulnerabilities without a careful analysis of

their effectiveness and their impact on interoperability.

During 2006, the United Kingdom's Centre for the Protection of National Infrastructure embarked itself in an ambitious and arduous project: performing a security assessment of the TCP and IP protocols and common implementation strategies. The project did not limit itself to an analysis of the relevant IETF specifications, but also included an analysis of common implementation strategies found in the most popular TCP and IP implementations. Additionally, it included a security assessment of new features, such as TCP window auto-tuning, that have been incorporated in a number of popular TCP/IP implementations, but whose security implications have never been thoroughly evaluated.

As strange as it may sound, this is the first thorough security assessment of the TCP and IP protocols and their common implementation strategies, and the first attempt to take much of the work the security community has done during the last 25 years to the IETF (Internet Engineering Task Force).

Extended Abstract

During the last twenty years, many vulnerabilities have been identified in the TCP/IP stacks of a number of systems. The discovery of these vulnerabilities led in most cases to reports being published by a number of CSIRTs and vendors, which helped to raise awareness about the threats and the best possible mitigations known at the time the reports were published.

For some reason, much of the effort of the security community on the Internet protocols did not result in official documents (RFCs) being issued by the organization in charge of the standardization of the communication protocols in use by the Internet: the Internet Engineering Task Force (IETF). This basically led to a situation in which "known" security problems have not always been addressed by all vendors. In addition, in many cases vendors have implemented quick "fixes" to the identified vulnerabilities without a careful analysis of their effectiveness and their impact on interoperability.

As a result, producing a secure TCP/IP implementation nowadays is a very difficult task, in large part because of the hard task of identifying relevant documentation and differentiating between that which provides correct advisory, and that which provides misleading advisory based on inaccurate or wrong assumptions.

During 2006, the United Kingdom's Centre for the Protection of National Infrastructure embarked itself in an ambitious and arduous project: performing a security assessment of the TCP and IP protocols. The project did not limit itself to an analysis of the relevant IETF specifications, but also included an analysis of common implementation strategies found in the most popular TCP and IP implementations. The result of the project was a set of documents which identifies possible threats for the TCP and IP protocols and, where possible, proposes counter-measures to mitigate the identified threats.

This presentation will will describe some of the new insights that were gained as a result of this project. Additionally, it will provide an overview of the state of affairs of the different TCP/IP implementations found in BSD operating systems.

Attached materials

"Security Assessment of the Internet Protocol", written by Fernando Gont on behalf of the United Kingdom's Centre for the Protection of National Infrastructure (CPNI). Published in July 2008. (available at: http://www.cpni.gov.uk/Docs/InternetProtocol.pdf)

"Security Assessment of the Transmission Control Protocol (TCP)", written by Fernando Gont on behalf of the United Kingdom's Centre for the Protection of National Infrastructure (CPNI). This document, of 140+ pages, is in publication process, and therefore has not been delivered to the Program Comitee.

Brief biography

Fernando Gont specializes in the field of communications protocols security, working for private and gubernamental organizations both in Argentina and overseas.

Gont has worked on a number of projects for the UK National Infrastructure Security Co-ordination Centre (NISCC) and the UK Centre for the Protection of National Infrastructure (CPNI) in the field of communications protocols security. As part of his work for these organizations, he has written a series of documents with recommendations for network engineers and implementers of the TCP/IP protocol suite.

Gont is a member of the Centro de Estudios de Informatica (CEDI) at Universidad Tecnológica Nacional/Facultad Regional Haedo (UTN/FRH) of Argentina, where he works in the field of Internet engineering.

He is active in several working groups of the Internet Engineering Task Force (IETF), where he has has published a number of IETF Internet-Drafts, most of which have already been adopted by the IETF for their future publication as Internet RFCs.

Gont has been a speaker at a number of conferences and technical meetings about information security, operating systems, and Internet engineering, including: CanSecWest 2005, BSDCan 2005, Midnight Sun Vulnerability and Security Workshop/Retreat 2005, FIRST Technical Colloquium 2005, IETF 64, IETF 67, IETF 72, LACNIC X, JCC 2007, y LACNIC XI.