DEEPSEC 2009 Proposal

Proposed presentation title:

Results of a Security Assessment of the TCP and IP Protocols and Common Implementation Strategies

Speaker:

Fernando Gont

Description:

Fernando Gont will present the results of a security assessment of the TCP and IP protocols carried out on behalf of the UK CPNI (United Kingdom's Centre for the Protection of National Infrastructure). He will explain the security implications arising from the protocol specifications themselves, and from a number of implementation strategies followed by most of the popular TCP/IP stacks, and will also discuss the new insights that were gained as a result of this project that can help to mitigate the aforementioned issues. Finally, Fernando will provide an overview of the ongoing efforts at the IETF community to incorporate these insights into the corresponding protocol specifications and the efforts in the vendor community to incorporate these recommendations into popular implementations of the protocols.

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 IETF specifications 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. Additionally, it included a security assessment of new features, such as TCP window auto-tuning, that have been recently incoporate in operating systems such as Windows Vista and FreeBSD, 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, the first security asessment of newly-incorporated mechanisms (such as TCP window auto-tuning), and the first attempt to take much of the work and wisdom of the security community to the IETF (Internet Engineering Task Force) and the vendor community.

Attached documents:

Gont, F., “Security Assessment of the Internet Protocol”. Published in July 2008 by the United Kingdom's Centre for the Protection of National Infrastructure.

Gont, F., “Security Assessment of the Transmission Control Protocol (TCP)”. Published in February 2009 by the United Kingdom's Centre for the Protection of National Infrastructure.

Fernando Gont's contact information & bio

e-mail:

fernando@gont.com.ar

web:

http://www.gont.com.ar

Cell-phone:

+54 9 11 6536 4380

Telephone:

+54 11 4464 5710

Postal address:

Evaristo Carriego 2644
1706, Haedo
Provincia de Buenos Aires
Argentina

Country of origin:

Argentina

Employer and/or affiliations:

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

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 working on security assessments of communications protocols on behalf of the United Kingdom's Centre for the Protection of National Infrastructure. Additionally, he 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. As part of his work, he is active in several working groups of the Internet Engineering Task Force (IETF). He has published a number of IETF RFCs, and has also authored a number of IETF Internet-Drafts, most of which have already been adopted by the IETF for their future publication as 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 73, LACNIC X, LACNIC XI, and JCC 2007.

List of publications:

Gont, F. “Blind Duplicate-ACK spoofing attacks against TCP”. Research project carried out on behalf of UK’s CPNI (United Kingdom’s Centre for the Protection of National Infrastructure). (to be published)

Eggert, L., Gont, F., “TCP User TimeOut (UTO) Option”. IETF RFC 5482. March 2009. Available at: http://tools.ietf.org/rfc/rfc5482.txt

Larsen, M., Gont, F. “Port Randomization”, IETF Internet Draft. March 2009. This document has been accepted as a working group item of the TSV WG (http://www.ietf.org/html.charters/tsvwg-charter.html). Available at: http://www.ietf.org/internet-drafts/draft-ietf-tsvwg-port-randomization-03.txt

Gont, F., “TCP’s Reaction to Soft Errors”. IETF RFC 5461. February 2009. Available at: http://tools.ietf.org/rfc/rfc5461.txt

Gont, F. “Security Assessment of the Transmission Control Protocol”. Research project carried out on behalf of UK’s CPNI (United Kingdom’s Centre for the Protection of National Infrastructure). Available at: http://www.cpni.gov.uk/Docs/tn-03-09-security-assessment-TCP.pdf

Gont, F. “Security Assessment of the Internet Protocol”. Research project carried out on behalf of UK’s CPNI (United Kingdom’s Centre for the Protection of National Infrastructure). July 2008. Available at: http://www.cpni.gov.uk/Docs/InternetProtocol.pdf

Gont, F., “Security Assessment of the Transmission Control Protocol (TCP)”, IETF Internet Draft. February 2009. Available at: http://www.ietf.org/internet-drafts/draft-gont-tcp-security-00.txt

Gont, F., “On the generation of TCP timestamps”, IETF Internet Draft. February 2009. Available at: http://www.ietf.org/internet-drafts/draft-gont-tcpm-tcp-timestamps-01.txt

Gont, F., Yourtchenko, A., “On the implementation of TCP urgent data”, IETF Internet Draft. February 2009. Available at: http://www.ietf.org/internet-drafts/draft-gont-tcpm-urgent-data-01.txt

Gont, F. “Security Assessment of the Internet Protocol version 4”, IETF Internet Draft. January 2009. This document has been accepted as a working group item of the OPSEC WG (http://www.ietf.org/html.charters/opsec-charter.html). Available at: http://www.ietf.org/internet-drafts/draft-ietf-opsec-ip-security-00.txt

Gont, F., Srisuresh, P., “Security implications of Network Address Translators (NATs)”, IETF Internet Draft. November 2008. Available at: http://www.ietf.org/internet-drafts/draft-gont-behave-nat-security-01.txt

Gont, F., “ICMP attacks against TCP”, IETF Internet Draft. October 2008. This document has been accepted as a working group item of the TCPM WG (http://www.ietf.org/html.charters/tcpm-charter.html). Available at: http://www.ietf.org/internet-drafts/draft-ietf-tcpm-icmp-attacks-04.txt

Gont, F., Gont, G., “Recommendations for filtering ICMP messages”, IETF Internet Draft. September 2008. This document has been accepted as a working group item of the OPSEC

WG (http://www.ietf.org/html.charters/opsec-charter.html). Available at: http://www.ietf.org/internet-drafts/draft-ietf-opsec-icmp-filtering-00.txt

“Improving TCP’s Resistance to Blind Attacks through Ephemeral Port Randomization”, Jornadas Chilenas de Computación 2007, Workshop de Sistemas Distribuidos y Paralelismo, November 2007.

Presentations:

“ICMP attacks”, CanSecWest 2005 Conference, May 2005, Vancouver, Canada.

“ICMP attacks against TCP”, BSDCan 2005 Conference, May 2005, Ottawa, Canada.

“ICMP attacks against TCP”, Midnight Sun Vulnerability and Security Workshop/Retreat 2005, June 2005, Hailuoto, Finland.

“ICMP attacks against TCP”, Forum of Incident Response and Security Teams Technical Colloquium (FIRST Technical Colloquium), October 5-7, 2005, Buenos Aires, Argentina.

“ICMP attacks against TCP”, 64th IETF Meeting, November 6-11, 2005, Vancouver, BC, Canada.

“TCP’s reaction to soft errors”, 64th IETF Meeting, November 6-11, 2005, Vancouver, BC, Canada.

“TCP User Timeout Option”, 64th IETF Meeting, November 6-11, 2005, Vancouver, BC, Canada.

“TCP UTO (User Timeout Option)”, 67th IETF Meeting, November 5-10, 2006, San Diego, CA, U.S.A.

“ICMP attacks against TCP”, 67th IETF Meeting, November 5-10, 2006, San Diego, CA, U.S.A.

“NAT Behavioral Requirements for ICMP”, 67th IETF Meeting, November 5-10, 2006, San Diego, CA, U.S.A.

“Mejoras de seguridad en TCP”, Evento de Seguridad Informática, LACNIC X, May 21-25, 2007, Isla Margarita, Venezuela.

“Ataques ICMP contra TCP”, Jornada de Seguridad Informática organizada por ANTEL, August 15, 2007. Montevideo, Uruguay.

“Randomización de puertos”, Jornada de Seguridad Informática organizada por ANTEL, August 15, 2007. Montevideo, Uruguay.

“Improving TCP’s Resistance to Blind Attacks through Ephemeral Port Randomization”, CACIC 2007, II Workshop de Arquitecturas, Redes y Sistemas Operativos, October 1-5, 2007. Corrientes y Resistencia, Argentina.

“Improving TCP’s Resistance to Blind Attacks through Ephemeral Port Randomization”, Jornadas Chilenas de Computación 2007, Workshop de Sistemas Distribuidos y Paralelismo, November 5-10, 2007. Iquique, Chile.

“Ataques ciegos contra TCP”, V Congreso Internacional de Computación Informática y Sistemas, November 12-16, 2007. Moquegua, Peru.

“Mejorando la resistencia de TCP a ataques ciegos mediante aleatorización de puertos efímeros”, V Congreso Internacional de Computación Informática y Sistemas, November 12-16, 2007. Moquegua, Peru.

“Mejorando la seguridad de TCP/IP mediante aleatorización de parámetros de protocolo”, ekoparty security conference, November 30th and December 1st, 2007. Buenos Aires, Argentina.

“Resultados de un análisis de seguridad de las especificaciones de la IETF de los protocolos TCP e IP”, LACNIC XI, May 26-30, 2008. Salvador de Bahia, Brazil.

“Resultados de un análisis de seguridad de los protocolos TCP e IP”, 5to Congreso Internacional de Ingeniería en Computación, Septiembre 23-26, 2008. Ixtlahuaca, Mexico.

“Servicios de directorio de Internet”, 5to Congreso Internacional de Ingeniería en Computación, Septiembre 23-26, 2008. Ixtlahuaca, Mexico.

“Resultados de un análisis de seguridad de los protocolos TCP e IP”, Congreso Seguridad en Cómputo 2008, Septiembre 19-26, 2008. Ciudad de México, México.

“Results of a Security Assessment of the TCP & IP Protocols”, ekoparty Security Conference - 4th edition, 2 y 3 de octubre, 2008. Buenos Aires, Argentina.

“Recommendations for filtering ICMP messages”, 73rd IETF Meeting, November 16-21, 2008. Minneapolis, MN, U.S.A.

“Security Assessment of the Internet Protocol version 4”, 73rd IETF Meeting, November 16-21, 2008. Minneapolis, MN, U.S.A.

“Port randomization”, 73rd IETF Meeting, November 16-21, 2008. Minneapolis, MN, U.S.A.

“On the implementation of TCP urgent data”, 73rd IETF Meeting, November 16-21, 2008. Minneapolis, MN, U.S.A.

“On the generation of TCP timestamps”, 73rd IETF Meeting, November 16-21, 2008. Minneapolis, MN, U.S.A.

“ICMP attacks against TCP”, 73rd IETF Meeting, November 16-21, 2008. Minneapolis, MN, U.S.A.

“Security Implications of Network Address Translators (NATs)”, 73rd IETF Meeting, November 16-21, 2008. Minneapolis, MN, U.S.A.

“Resultados de un análisis de seguridad de los protocolos TCP e IP”, 4ta Jornada de Seguridad Informática, November 25, 2008. Paraná, Entre Ríos, Argentina.