BSDCan 2010 Proposal

Proposed presentation title:

Security Implications of the Internet Protocol version 6 (IPv6)

Speaker:

Fernando Gont

Description

Fernando Gont will discuss some of the results of a Security Assessment of the Internet Protocol version 6 (IPv6) carried out on behalf of the UK CPNI (United Kingdom's Centre for the Protection of National Infrastructure). He will explain some of the security implications arising from the protocol specifications themselves, and from a number of implementation strategies followed by some of the most popular IPv6 implementations (including KAME). He will describe ongoing efforts to mitigate the aforementioned issues, and will explain the different system knobs that are available in the different BSD-flavours to control different aspects of the IPv6 stack.

Reason why this material is innovative or significant:

The IPv6 protocol suite was designed to accommodate the present and future growth of the Internet, by providing a much larger address space than that of its IPv4 counterpart, and is expected to be the successor of the original IPv4 protocol suite. It has already been deployed in a number of production environments, and many organizations have already scheduled or planned its deployment in the next few years.

There are a number of factors that make the IPv6 protocol suite interesting from a security standpoint. Firstly, being a new technology, technical personnel has much less confidence with the IPv6 protocols than with their IPv4 counterpart, and thus it is more likely that the security implications of the protocols be overlooked when they are deployed. Secondly, IPv6 implementations are much less mature than their IPv4 counterparts, and thus it is very likely that a number of vulnerabilities will be discovered in them before their robustness can be compared to that of the existing IPv4 implementations. Thirdly, there is much less implementation experience with the IPv6 protocols than with their IPv4 counterpart, and “best current practices” for their implementation are not available. Fourthly, security products such as firewalls and NIDS’s (Network Intrusion Detection Systems) usually have less support for the IPv6 protocols than for their IPv4 counterparts.

While a number of papers have been published on the security aspects of the IPv6 protocol suite, they usually provide general discussion on the security implications of IPv6, but do not delve into much detail regarding the security implications of each of the mechanisms, header fields, and options of all the involved protocols.

There is a clear need to raise awareness about the security aspects and implications of the IPv6 protocol suite, to improve the confidence of both IPv6 implementers and the personnel working on the deployment of IPv6 in production environments.

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 4650 8472

Postal address:
Evaristo Carriego 2644
1706, Haedo
Provincia de Buenos Aires
Argentina

Country of origin:
Argentina

Employer and/or affiliations:
Universidad Tecnológica Nacional/Facultad Regional Haedo (Argentina).
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 currently working on the security assessment 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), and has published a number of IETF Internet-Drafts and RFCs (Request For Comments). He currently leads the first IETF effort to improve the security of the TCP and the IPv4 protocols and their implementations.

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, BSDCan 2009, Midnight Sun Vulnerability and Security Workshop/Retreat 2005, FIRST Technical Colloquium 2005, Kernel Conference Australia 2009, DEEPSEC 2009, HACK.LU 09, IETF 64, IETF 67, IETF 73, IETF 76, LACNIC X,

LACNIC XI, and LACNIC XII.

List of publications:

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. “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).

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

Eggert, L., Gont, F., “TCP User TimeOut (UTO) Option”, IETF RFC 5482. March 2009. Available at: http://tools.ietf.org/rfc/rfc5489.txt

Gont, F. “Security Assessment of the Transmission Control Protocol (TCP)”, IETF Internet Draft. August 2009. 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-tcp-security-00.txt

Larsen, M., Gont, F. “Port Randomization”, IETF Internet Draft. November 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-05.txt

Gont, F. “Security Assessment of the Internet Protocol version 4”, IETF Internet Draft. August 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-01.txt

Gont, F., “ICMP attacks against TCP”, IETF Internet Draft. January 2010. 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-10.txt

Gont, F., Gont, G., “Recommendations for filtering ICMP messages”, IETF Internet Draft. October 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-icmp-filtering-01.txt

Gont, F., “On the generation of TCP timestamps”, IETF Internet Draft. September 2009. Available at: http://www.ietf.org/internet-drafts/draft-gont-tcpm-tcp-timestamps-02.txt

Gont, F., Yourtchenko, A., “On the implementation of TCP urgent data”, IETF Internet Draft. November 2009. 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-urgent-data-02.txt

Gont, F., Srisuresh, P., "Security implications of Network Address Translators (NATs)", IETF Internet Draft. October 2009. Available at: http://www.ietf.org/internet-drafts/draft-gont-behave-nat-security-03.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.

“Results of a Security Assessment of the TCP and IP protocols and Common Implementation Strategies”, BSDCan 2009 Conference, May 8-9, 2009. Ottawa, Canada.

“Security Assessment of the Transmission Control Protocol (TCP)”, LACNIC XII, May 25-29, 2009. Panama City, Panama.

“Security Assessment of the Internet Protocol (IP)”, LACNIC XII, May 25-29, 2009. Panama City, Panama.

“Security Assessment of Common Implementation Strategies of the TCP and IP Protocols”, Kernel Conference Australia 2009, July 15-17, 2009. Brisbane, Australia.

“Some insights about the recent TCP DoS (Denial of Service) vulnerabilities”, HACK.LU 09 Conference, October 28-30, 2009. Luxembourg.

“Ongoing work at the IETF on TCP and IP security” (lightning talk), HACK.LU 09 Conference, October 28-30, 2009. Luxembourg.

“TCP for DNS security considerations”, 76th IETF Meeting, November 9-13, 2009. Hiroshima, Japan.

“Security Assessment of the Internet Protocol version 4”, 76th IETF Meeting, November 9-13, 2009. Hiroshima, Japan

“Recommendations for filtering ICMP messages”, 76th IETF Meeting, November 9-13, 2009. Hiroshima, Japan.

“Security Implications of Network Address Translators (NATs)”, 76th IETF Meeting, November 9-13, 2009. Hiroshima, Japan.

“Results of a Security Assessment of the TCP and IP Protocols and Common Implementation Strategies”, DEEPSEC 2009, November 18-20, 2009. Vienna, Austria.