Training: IPv6 Hacking Crash Course

Instructor: Fernando Gont

Overview

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. The imminent exhaustion of the IPv4 address space has resulted in the deployment of IPv6 in a number of production environments, with many other organizations planning to deploy IPv6 in the short or near term.

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 the protocols 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 matches that of the existing IPv4 implementations. Thirdly, 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. Fourthly, the security implications of IPv6 transition/co-existence technologies on existing IPv4 networks are usually overlooked, potentially enabling attackers to leverage these technologies to circumvent IPv4 security measures in unexpected ways.

The imminent global deployment of IPv6 has created a global need for security professionals with expertise in the field of IPv6 security, such that the aforementioned security issues can be mitigated.

IPv6 Hacking Crash Course provides a full-day intense IPv6 hacking experience, focusing on hands-on IPv6 hacking exercises. The training is carried out by **Fernando Gont**, a world-renowned IPv6 security expert.

Learning Objectives

This course will provide the attendee with a full-day intense IPv6 hacking experience, focusing on hands-on IPv6 hacking exercises. IPv6 theory is reduced to a minimum, and participants are guided through a series of hands-on exercises ranging from IPv6 network reconnaissance to a number of IPv6-based Denial of Service attacks.

This course will employ a range of open source tools to evaluate the security of IPv6 networks, and to provide live demos of many IPv6 vulnerabilities. During the course, the attendee will perform a large number of exercises in a network laboratory (with the assistance of the trainer) and on the public IPv6 Internet, to get a real experience of what IPv6 security is all about.

Who Should Attend

Network Engineers, Network Administrators, Security Administrators, Penetration Testers, and Security Professionals in general.

Participants Are Required To

Participants are required to have a good understanding of the IPv4 protocol suite (IPv4, ICMP, etc.) and of related components (routers, firewalls, etc.). Additionally, the attendee is expected to knowledge about basic IPv4 troubleshooting tools, such as: ping, traceroute, and network protocol analyzers (e.g., tcpdump). Some basic IPv6 knowledge is desirable, but not required.

What to bring

Attendees willing to perform the hands-on exercises are expected to bring a laptop with VirtualBox already installed, and an empty memory stick (of at least 4 GB) or CD/DVD drive. The minimum requirements for the laptop are: Intel Core Duo, 1.66 GHz. 1GB of RAM. Ethernet and WI-FI network interface cards.

Course Length

1 day

Topics covered by this course

- Brief Introduction to IPv6
- Address scanning in IPv6
- IPv6 Extension Headers and IPv6 Options for fun and profit
- ICMPv6 for network reconnaissance
- IPv6 Neighbor Discovery Attacks
- Stateless Address Auto-configuration (SLAAC) Attacks
- Dynamic Host Configuration Protocol version 6 (DHCPv6) attacks
- DNS tricks for IPv6
- IPv6 firewalls
- Playing with IPv6 Transition/co-existence technologies (6to4, Teredo, ISATAP, etc.)
- Network reconnaissance in IPv6
- VPN-leakages in dual-stack and IPv4-only networks
- Security Implications of IPv6 on IPv4-only networks
- Miscellaneous topics

About the Instructor

Fernando Gont is a security researcher and consultant at SI6 Networks (http://www.si6networks.com).

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, and has performed the first thorough security assessment of the IPv6 protocol suite.

Gont is currently working as a security consultant and researcher for SI6 Networks, leading IPv6 standardization activities in the area of IPv6 security, and working on IPv6 vulnerability research. 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 RFCs (Request For Comments) and Internet-Drafts. Additionally, he has produced the SI6 Network's IPv6 toolkit (http://www.si6networks.com/tools): a free software, portable, and comprehensive IPv6 toolkit for security assessment and trouble-shooting of IPv6 networks and 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, Midnight Sun Vulnerability and Security Workshop/Retreat 2005, FIRST Technical Colloquium 2005, Kernel Conference Australia 2009, DEEPSEC 2009, HACK.LU 09, HACK.LU 2011, DEEPSEC 2011, LACSEC 2012, Hackito Ergo Sum 2012, and Hack In Paris 2012.

More information about Fernando Gont is available at his personal web site: <http://www.gont.com.ar>.

Fernando Gont's contact information & bio

e-mail:
fgont@si6networks.com || fernando@gont.com.ar

web:
http://www.si6networks.com || http://www.gont.com.ar

Linkedin Profile:
http://www.linkedin.com/in/fernandogont

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:
SI6 Networks

Brief biography:

Fernando Gont is a security researcher and consultant at SI6 Networks (http://www.si6networks.com).

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, and has performed the first thorough security assessment of the IPv6 protocol suite.

Gont is currently working as a security consultant and researcher for SI6 Networks, leading IPv6 standardization activities in the area of IPv6 security, and working on IPv6 vulnerability research. 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 RFCs (Request For Comments) and Internet-Drafts. Additionally, he has produced the SI6 Network's IPv6 toolkit (http://www.si6networks.com/tools): a free software, portable, and comprehensive IPv6 toolkit for security assessment and trouble-shooting of IPv6 networks and 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, Midnight Sun Vulnerability and Security Workshop/Retreat 2005, FIRST Technical Colloquium 2005, Kernel Conference Australia 2009, DEEPSEC 2009, HACK.LU 09, HACK.LU 2011, DEEPSEC 2011, LACSEC 2012, Hackito Ergo Sum 2012, and Hack In Paris 2012.

More information about Fernando Gont is available at his personal web site: <http://www.gont.com.ar>.

List of publications:

Technical Reports

Gont, F. "Security Assessment of IPv6 Neighbor Discovery Implementations" (whitepaper). Project carried out for SI6 Networks. Available at: http://www.si6networks.com/tools/ipv6toolkit/si6networks-ipv6-nd-assessment.pdf

Gont, F. "Security Assessment of the Internet Protocol version 6 (IPv6)". Research project carried out on behalf of the UK's CPNI (United Kingdom's Centre for the Protection of National Infrastructure). (available on request).

Gont, F. "Security Assessment of the Transmission Control Protocol". Research project carried out on behalf of the UK's CPNI (United Kingdom's Centre for the Protection of National Infrastructure). Available at: http://www.gont.com.ar/papers/tn-03-09-security-assessment-TCP.pdf

Gont, F. "Security Assessment of the Internet Protocol". Research project carried out on behalf of the UK's CPNI (United Kingdom's Centre for the Protection of National Infrastructure). July 2008. Available at: http://www.gont.com.ar/papers/InternetProtocol.pdf

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

Gont, F. "Advice on FICORA #193744". Research project carried out on behalf of the UK's CPNI (United Kingdom's Centre for the Protection of National Infrastructure).

IETF RFCs

Pignataro, C., Gont, F., "Formally Deprecating some IPv4 Options", IETF RFC 6814. November 2012. Available at: http://www.rfc-editor.org/rfc/rfc6814.txt

Gont, F. "Deprecation of ICMP Source Quench messages", IETF RFC 6633. May 2012. Available at: http://www.rfc-editor.org/rfc/rfc6633.txt

Gont, F., Bellovin, S., “Defending Against Sequence Number Attacks”, IETF RFC 6528. February 2012. Available at: http://www.rfc-editor.org/rfc/rfc6528.txt

Gont, F. “Security Assessment of the Internet Protocol version 4”, IETF RFC 6274. July 2011. Available at: http://www.rfc-editor.org/rfc/rfc6274.txt

Gont, F., “Reducing the TIME-WAIT state using TCP timestamps”, IETF RFC 6191. April 2011. Available at: http://www.rfc-editor.org/rfc/rfc6191.txt

Larsen, M., Gont, F. “Transport Protocol Port Randomization Recommendations”, IETF RFC 6056. Available at: http://www.rfc-editor.org/rfc/rfc6056.txt

Gont, F., Yourtchenko, A., “On the implementation of TCP urgent data”, IETF RFC 6093. January 2011. Available at: http://www.rfc-editor.org/rfc/rfc6093.txt

Gont, F., “ICMP attacks against TCP”, IETF RFC 5927. July 2010. Available at: http://www.rfc-editor.org/rfc/rfc5927.txt

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

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

IETF Internet-Drafts (working group items)

Gont, F., Chown, T., “Network Reconnaissance in IPv6 Networks”, IETF Internet Draft, December 2012. 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://tools.ietf.org/id/draft-ietf-opsec-ipv6-host-scanning-00.txt

Gont, F., “Virtual Private Network (VPN) traffic leakages in dual-stack hosts/networks”, IETF Internet-Draft, December 2012. 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://tools.ietf.org/id/draft-ietf-opsec-vpn-leakages-00.txt

Gont, F., Liu, W., Van de Velde, G., “DHCPv6-Shield: Protecting Against Rogue DHCPv6 Servers”, IETF Internet Draft. December 2012. 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://tools.ietf.org/id/draft-ietf-opsec-dhcpv6-shield-00.txt

Gont, F., “Security Implications of IPv6 on IPv4 Networks”, IETF Internet Draft, December 2012. 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://tools.ietf.org/html/draft-ietf-opsec-ipv6-implications-on-ipv4-nets

Gont, F., “Processing of IPv6 'atomic' fragments”, IETF Internet Draft, August 2012. This document has been accepted as a working group item of the 6man WG (http://www.ietf.org/html.charters/6man-charter.html). Available at: http://www.ietf.org/internet-drafts/draft-ietf-6man-ipv6-atomic-fragments-01.txt

Gont, F., “A method for Generating Stable Privacy-Enhanced Addresses with IPv6 Stateless Address Autoconfiguration (SLAAC)”, IETF Internet Draft, May 2012. This document has been accepted as a working group item of the 6man WG (http://www.ietf.org/html.charters/6man-charter.html). Available at: http://www.ietf.org/internet-drafts/draft-ietf-6man-stable-privacy-addresses-00.txt

Gont, F., Manral, V., “Security and Interoperability Implications of Oversized IPv6 Header Chains”, IETF Internet Draft, August 2012. This document has been accepted as a working group item of the 6man WG (http://www.ietf.org/html.charters/6man-charter.html). Available at: http://www.ietf.org/internet-drafts/draft-ietf-6man-oversized-header-chain-02.txt

Gont, F., “Security Implications of the Use of IPv6 Extension Headers with IPv6 Neighbor Discovery”, IETF Internet Draft, June 2012. This document has been accepted as a working group item of the 6man WG (http://www.ietf.org/html.charters/6man-charter.html). Available at: http://www.ietf.org/internet-drafts/draft-ietf-6man-nd-extension-headers-03.txt

Gont, F., “Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard)”, IETF Internet Draft, August 2012. This document has been accepted as a working group item of the v6ops WG (http://www.ietf.org/html.charters/v6ops-charter.html). Available at: http://www.ietf.org/internet-drafts/draft-ietf-v6ops-ra-guard-implementation-05.txt

Gont, F., Gont, G., C. Pignataro, “Recommendations for filtering ICMP messages”, IETF Internet Draft. March 2012. 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-03.txt

Gont, F., Atkinson, R., Pignataro, C., “IP Options Filtering Recommendations”, IETF Internet Draft, June 2012. 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-options-filtering-00.txt

IETF Internet-Drafts (individual submissions)

Gont, F. “Security Assessment of Neighbor Discovery (ND) for IPv6”. IETF Internet-Draft, November 2012. Available at: http://tools.ietf.org/html/draft-gont-opsec-ipv6-nd-security

Gont, F., “Interoperability Problems of StateLess Address Auto-Configuration (SLAAC) Arising from Duplicate Link-layer Addresses”, IETF Internet-Draft, October 2012. Available at: http://tools.ietf.org/html/draft-gont-v6ops-slaac-issues-with-duplicate-macs

Gont, F., “Obsoleting the Endpoint Identifier (EID) Option”, IETF Internet Draft. October 2012. Available at: http://www.ietf.org/internet-drafts/draft-gont-intarea-obsolete-eid-option-01.txt

Gont, F., “Processing of TCP segments with Mirrored End-points”, IETF Internet Draft, March 2012. Available at: http://www.ietf.org/internet-drafts/draft-gont-tcpm-tcp-mirrored-endpoints-00.txt

Gont, F., “Processing of IP Security/Compartment and Precedence Information by TCP”, IETF Internet Draft, March 2012. Available at: http://www.ietf.org/internet-drafts/draft-gont-tcpm-tcp-seccomp-prec-00.txt

Gont, F., “Recommendations for IPv6 Firewall Design and Implementation”, IETF Internet Draft, January 2012. (available on request).

Gont, F., “Security Assessment of the IPv6 Flow Label”, IETF Internet Draft, January 2012. Available at: http://www.ietf.org/internet-drafts/draft-gont-6man-flowlabel-security-02.txt

Gont, F., “Security Implications of Predictable Fragment Identification Values”, IETF Internet Draft, March 2012. Available at: http://www.ietf.org/internet-drafts/draft-gont-6man-predictable-fragment-id-02.txt

Gont, F., “Security Implications of IPv6 options of Type 10xxxxxx”, IETF Internet Draft, December 2011. Available at: http://www.ietf.org/internet-drafts/draft-gont-6man-ipv6-smurf-amplifier-00.txt

Gont, F., “Managing the Address Generation Policy for Stateless Address Autoconfiguration in IPv6”, IETF Internet Draft, December 2011. Available at: http://www.ietf.org/internet-drafts/draft-gont-6man-managing-slaac-policy-00.txt

Gont, F., “Neighbor Discovery Shield (ND-Shield): Protecting against Neighbor Discovery Attacks”, IETF Internet Draft. June 2012. Available at: http://tools.ietf.org/id/draft-gont-opsec-ipv6-nd-shield-00.txt

Gont, F., Simerda, P., “Current issues with DNS Configuration Options for SLAAC”, IETF Internet Draft. June 2012. Available at: http://tools.ietf.org/id/draft-gont-6man-slaac-dns-config-issues-00.txt

Gont, F., “Security Implications of IPv6 options of Type 10xxxxxx”, IETF Internet Draft, December 2011. Available at: http://tools.ietf.org/id/draft-gont-6man-ipv6-smurf-amplifier-00.txt

Gont, F., “IPv6 Router Advertisement Guard (RA-Guard) Evasion”, IETF Internet Draft, June 2011. Available at: http://tools.ietf.org/id/draft-gont-v6ops-ra-guard-evasion-01.txt

Gont, F. “Security Assessment of the Transmission Control Protocol (TCP)”, IETF Internet Draft. January 2011. Available at: http://www.ietf.org/internet-drafts/draft-ietf-tcpm-tcp-security-02.txt

Gont, F., “On the Specification of IPv6 Extension Headers”, IETF Internet Draft, January 2011. Available at: http://www.ietf.org/id/draft-gont-6man-extension-headers-00.txt

Gont, F., “Mitigating Teredo Routing Loop Attacks”, IETF Internet Draft, September 2010. Available at: http://www.ietf.org/internet-drafts/draft-gont-6man-teredo-loops-00.txt

Gont, F., “Moving the Endpoint Identifier (EID) Option to Obsolete Status”, IETF Internet Draft, August 2010. Available at: http://www.ietf.org/internet-drafts/draft-gont-6man-obsolete-eid-option-00.txt

Gont, F., Oppermann, A., “On the generation of TCP timestamps”, IETF Internet Draft, June 2010. Available at: http://www.ietf.org/internet-drafts/draft-gont-timestamps-generation-00.txt

Kristoff, J., O'Reirdan, M., Gont, F., “Port Filtering Considerations”, IETF Internet Draft, March 2010. Available at: http://www.ietf.org/internet-drafts/draft-kristoff-opsec-port-filtering-00.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., 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

Gont, F., “Increasing the payload of ICMP error messages”, IETF Internet Draft. August 2004. Available at: http://www.ietf.org/internet-drafts/draft-gont-icmp-payload-00.txt

Gont, F., “TCP Adaptive User TimeOut (AUTO) Option”, IETF Internet Draft. May 2004. Available at: http://www.ietf.org/internet-drafts/draft-gont-tcpm-tcp-auto-option-00.txt

Gont, F., “On the problem of long delays between connection-establishment attempts”, IETF Internet Draft. January 2009. Available at: http://www.ietf.org/internet-drafts/draft-gont-tcpm-connection-delays-00.txt

Refereed Papers

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

Gont, F., “Improving TCP’s Resistance to Blind Attacks through Ephemeral Port Randomization”, CACIC 2007, II Workshop de Arquitecturas, Redes y Sistemas Operativos, Octtober 2007.

Magazine Articles

Gont, F. “A vulnerability in the Path-MTU Discovery mechanism”, Revista hackin9 (edición en inglés), Editorial Software-Wydawnictwo Sp.z.o.o, Polond. August 2007.

Gont, F. “Ataque contra el mecanismo ‘Path-MTU Discovery’”, Revista hackin9 (edición en español), Editorial Software-Wydawnictwo Sp.z.o.o, Poland. July 2007.

Gont, F. “ICMP-based blind connection-reset attack”, Revista hackin9 (edición en Inglés), Editorial Software-Wydawnictwo Sp.z.o.o, Poland. July 2007.

Gont, F. “Ataque ‘Blind connection-reset’ basado en ICMP”, Revista hackin9 (edición en español), Editorial Software-Wydawnictwo Sp.z.o.o, Poland. June 2007.

Gont, F. “Randomización de puertos TCP efímeros”, Revista @rroba, Editorial Megamultimedia, Spain. May 2007.

Gont, F. “Ataques de reseteo de conexión contra TCP”, Revista @rroba, Editorial Megamultimedia, Spain. March 2007.

Gont, F. “Trucos con el campo ‘Identificación’ del Protocolo de Internet (IP)”, Revista @rroba, Editorial Megamultimedia, Spain. December 2006.

Gont, F. “Escaneo anónimo de puertos”, Revista @rroba, Editorial Megamultimedia, Spain. October 2006.

Gont, F. “Evasión de Sistemas de Detección de Intrusos en Red”, Revista @rroba, Editorial Megamultimedia, Spain. July 2006.

Gont, F. “Sniffeando redes con tcpdump (tercera parte)”, Revista @rroba, Editorial Megamultimedia, Spain. March 2006.

Gont, F. “Sniffeando redes con tcpdump (segunda parte)”, Revista @rroba, Editorial Megamultimedia, Spain. February 2006.

Gont F., “Sniffeando redes con tcpdump (primera parte)”, Revista @rroba, Editorial MegaMultimedia, Spain. January 2006.

Gont F., “La política detrás de las vulnerabilidades”, Revista @rroba, Editorial MegaMultimedia, Spain. December 2005.

Gont F., “Investigando el Sistema de Nombres de Dominio (DNS)”, Revista @rroba, Editorial MegaMultimedia, Spain. September 2005.

Gont F., “El Sistema de Nombres de Dominio (DNS)”, Revista @rroba, Editorial MegaMultimedia, Spain. August 2005.

Gont F., “El servicio ‘whois’”, Revista @rroba, Editorial MegaMultimedia, Spain. Julio 2005.

Gont F., “Rastreando spammers”, Revista @rroba, Editorial MegaMultimedia, Spain. June 2005.

Gont F., “El ataque SYN-flood”, Revista @rroba, Editorial MegaMultimedia, Spain. May 2005.

Gont F., “El ataque contra el mecanismo Path-MTU Discovery”, Revista @rroba, Editorial MegaMultimedia, Spain. April 2005.

Gont, F., “El ataque ‘ICMP Source Quench’”, Revista @rroba, Editorial MegaMultimedia, Spain. March 2005.

Gont, F., “El ataque ‘blind connection-reset’”, Revista @rroba, Editorial MegaMultimedia, Spain. February 2005.

Web portal articles

Gont, F., “Analysis: Vast IPv6 address space actually enables IPv6 attacks”, TechTarget's SearchSecurity.com Portal. June 2012. Available at: http://searchsecurity.techtarget.com/tip/Analysis-Vast-IPv6-address-space-actually-enables-IPv6-attacks

Gont, F., “IPv6 First Hop Security”, TechTarget's SearchEnterpriseWAN.com Portal, January 2012. Available at: http://searchenterprisewan.techtarget.com/tip/First-hop-security-in-IPv6

Gont, F., “IPv6 firewall security: Fixing issues introduced by the new protocol”, TechTarget's SearchEnterpriseWAN.com Portal, November 2011. Available at: http://searchenterprisewan.techtarget.com/tip/IPv6-firewall-security-Fixing-issues-introduced-by-the-new-protocol

Gont, F., “Requirements for secure IPv6 deployments include better IPv6 tester tools”, TechTarget's SearchSecurity.com Portal. July 2011. Available at: http://searchsecurity.techtarget.com/tip/Requirements-for-secure-IPv6-deployments-include-better-IPv6-tester-tools

Gont, F., “IPv6 security issues: IPv6 transition mechanisms”, TechTarget's SearchSecurity.com Portal. June 2011. Available at: http://searchsecurity.techtarget.com/tip/IPv6-security-issues-IPv6-transition-mechanisms

Gont, F., “IPv6 myths: Debunking misconceptions regarding IPv6 security features”, TechTarget's SearchSecurity.com Portal. May 2011. Available at: http://searchsecurity.techtarget.com/tip/IPv6-myths-Debunking-misconceptions-regarding-IPv6-security-features

Gont, F., “Why IPv6 won't rid the Internet of Network Address Translation”, TechTarget's SearchEnterpriseWAN.com Portal, January 2011. Available at: http://searchenterprisewan.techtarget.com/tip/Why-IPv6-wont-rid-the-Internet-of-Network-Address-Translation

Talks:

“DHCPv6-Shield: Protecting Against Rogue DHCPv6 Servers”. IETF 85. November 4-9, 2012. Atlanta, GA, USA.

“Virtual Private Network (VPN) traffic leakages in dual-stack hosts/networks”. IETF 85. November 4-9, 2012. Atlanta, GA, USA.

“Network Reconnaissance in IPv6 Networks”. IETF 85. November 4-9, 2012. Atlanta, GA, USA.

“Virtual Private Network (VPN) traffic leakages in dual-stack hosts/networks”. IETF 85. November 4-9, 2012. Atlanta, GA, USA.

“IPv6 Toolkit: Security Assessment and Trouble-shooting of IPv6 networks”. IEPG 85. November 4, 2012. Atlanta, GA, USA.

“IPv6 Toolkit: Security Assessment and Trouble-shooting of IPv6 networks” (lightning talk, in Spanish). LACNOG 2012. October 28-November 1, 2012. Montevideo, Uruguay.

“La vida de un IETF Internet Draft (lightning talk, en Español). LACNOG 2012. October 28-November 1, 2012. Montevideo, Uruguay.

“Recent Advances in IPv6 Security”. H2HC 2012. October 20-21, 2012. Sao Paulo, Brazil.

“Seguridad IPv6”. WALC 2012, track “Despliegue de IPv6”. October 15-19, 2012. Panama City, Panama.

“Recent Advances in IPv6 Security”. SecTor 2012. October 8-9, 2012. Toronto, Canada.

“Recent Advances in IPv6 Security”. BruCON 2012. September 26-27, 2012. Ghent, Belgium.

“Hacking IPv6 Networks” (training). BruCON 2012. September 24-25, 2012. Ghent, Belgium.

“Seguridad IPv6: Ataque y Defensa”. Campus Party Quito 2012. September 19-23, 2012. Quito, Ecuador.

“IPv6: Motivación y Desafíos”. Campus Party Quito 2012. September 19-23, 2012. Quito, Ecuador.

“Resultados de un Análisis de Seguridad de IPv6”. FIRST Technical Colloquium 2012, August 30-31, 2012. Buenos Aires, Argentina.

“Seguridad IPv6: mitos y realidades”. Conferencia ADACSI, August 23, 2012. Buenos Aires, Argentina.

“Current Issues with DNS Configuration Options for SLAAC”. IETF 84, July 29-August 3, 2012. Vancouver, Canada.

“Managing the Address Generation Policy for Stateless Address Autoconfiguration in IPv6”. IETF 84, July 29-August 3, 2012. Vancouver, Canada.

“Security Implications of Predictable Fragment Identification Values”. IETF 84, July 29-August 3, 2012. Vancouver, Canada.

“DHCPv6-Shield: Protecting Against Rogue DHCPv6 Servers”. IETF 84, July 29-August 3, 2012. Vancouver, Canada.

“Host Scanning in IPv6 Networks”. IETF 84, July 29-August 3, 2012. Vancouver, Canada.

“Security Implications of IPv6 on IPv4 Networks”. IETF 84, July 29-August 3, 2012. Vancouver, Canada.

“ND-Shield: Protecting against Neighbor Discovery Attacks”. IETF 84, July 29-August 3, 2012. Vancouver, Canada.

“Recent Advances in IPv6 Security”. Just4Meeting 2012 Conference. July 6-8, 2012. Lisbon, Portugal.

“Hacking IPv6 Networks” (training). Hack In Paris 2012 Conference. June 18-20, 2012. Paris, France.

“Results of a Security Assessment of the Internet Protocol version 6 (IPv6)”. Hack In Paris 2012, June 18-22, 2012. Paris, France.

“Introducción y Experiencias en el IETF”. Lanzamiento Mundial de IPv6 - Mendoza, June 6, 2012. Ciudad de Mendoza, Argentina.

“Seguridad IPv6”. Lanzamiento Mundial de IPv6 - Mendoza, June 6, 2012. Ciudad de Mendoza, Argentina.

“Recent Advances in IPv6 Security”. BSDCan 2012, May 11-12, 2012. Ottawa, Canada.

“IPv6 Network Reconnaissance”. LACSEC 2012, LACNIC XVII, Mayo 6-11, 2012. Quito, Ecuador.

“IPv6 First Hop Security”. FLIP6, LACNIC XVII, May 6-11, 2012. Quito, Ecuador.

“Recent Advances in IPv6 Security”. Hackito Ergo Sum 2012, April 12-14, 2012. Paris, France.

“Generating Stable Privacy-Enhanced Addresses with IPv6 SLAAC”. IETF 83, March 25-30, 2012. Paris, France.

“Security Implications of Predictable Fragment Identification Values”. IETF 83, March 25-30, 2012. Paris, France.

“Security Implications of the Use of IPv6 Extension Headers with Neighbor Discovery”. IETF 83, March 25-30, 2012. Paris, France.

“Security and Interoperability Implications of Oversized IPv6 Header Chains”. IETF 83, March 25-30, 2012. Paris, France.

“Managing the Address Generation Policy for Stateless Address Autoconfiguration in IPv6”. IETF 83, March 25-30, 2012. Paris, France.

“Implementation Advice for RA-Guard”. IETF 83, March 25-30, 2012. Paris, France.

“Filtering of IPv4 packets containing IPv4 Options”. IETF 83, March 25-30, 2012. Paris, France.

“Recommendations for filtering ICMP messages”. IETF 83, March 25-30, 2012. Paris, France.

“Aspectos de Seguridad IPv6”. Campus Party 2012, February 10, 2012. Sao Paulo, Brazil.

“Managing the Use of Privacy Extensions for SLAAC in IPv6”. 80th IETF Meeting, March 27-April 1, 2011. Prague, Czech Republic.

“Security Assessment of the Transmission Control Protocol (TCP)”. 80th IETF Meeting, March 27-April 1, 2011. Prague, Czech Republic.

“Defending Against Sequence Number Attacks”. 80th IETF Meeting, March 27-April 1, 2011. Prague, Czech Republic.

“Seguridad IPv6”. Virtual seminar organized by LACNIC, April 29, 2011. Buenos Aires, Argentina.

“Tutorial: Seguridad IPv6”. Tutorial. LACNIC XV, May 15-20, 2011. Cancun, Mexico.

“Results of a Security Assessment of Neighbor Discovery (ND) for IP version 6 (IPv6)”. LACSEC 2011, May 17, 2011. Cancun, Mexico.

“Resultados de un análisis de seguridad de IPv6”. CONATEL 2011, May 17-20, 2011. Arequipa, Peru.

“Análisis de Seguridad de 'Descubrimiento de Vecinos' (Neighbor Discovery) para IPv6”. Cisco Academy Conference 2011, May 21, 2011. Arequipa, Peru.

“Security Implications of the Internet Protocol version 6 IPv6)”. UK IPv6 Transition Workshop. May 27, 2011, London, United Kingdom.

“Hacking IPv6 Networks” (training). Hack In Paris 2011. June 14-17, 2011, Paris, France.

“Seguridad IPv6”. Cisco Seminars: IPv6 Migration. July 1, 2011. Buenos Aires, Argentina.

“Seguridad IPv6”. Jornadas Técnicas ARIU 2011. September 2, 2011. Buenos Aires, Argentina.

“Results of a Security Assessment of the Internet Protocol version 6 (IPv6)”. HACK.LU 2011 Conference, September 19-21, 2011. Luxembourg, Grand Duchy of Luxembourg.

“Seguridad IPv6” (tutorial, in Spanish). LACNOG 2011, October 3-7, 2011. Buenos Aires, Argentina.

“Neighbor Discovery para IPv6: Ataques y Contramedidas”. LACNOG 2011, October 3-7, 2011. Buenos Aires, Argentina.

“Seguridad IPv6” (tutorial, in Spanish). WALC 2011 (IPv6 Protocol Track), October 10-14, 2011. Guayaquil, Ecuador.

“Seguridad IPv6” (tutorial, in Spanish). WALC 2011 (Security Track), October 10-14, 2011. Guayaquil, Ecuador.

“Resultados de un análisis de seguridad de IPv6”. CIICT 2011, October 25-28, 2011. Tunja, Colombia.

“Results of a Security Assessment of the Internet Protocol version 6 (IPv6)”. H2HC 2011 Conference, October 29-30, 2011. Sao Paulo, Brazil.

“Hacking IPv6 Networks” (training). DEEPSEC 2011 Conference, November 15-18, 2011. Vienna, Austria.

“Results of a Security Assessment of the Internet Protocol version 6 (IPv6)”. DEEPSEC 2011 Conference, November 15-18, 2011. Vienna, Austria.

“Seguridad IPv6”. Congreso Seguridad en Cómputo 2011, November 18-25. Mexico City, Mexico.

“IPv6: Historia, Presente, y Futuro”. 1HackParaLosChicos – Edicion N°2, December 14, 2011. Buenos Aires, Argentina.

“The Truth about IPv6 Security”. Future-Net 2010, May 10-13, 2010, Boston, MA, U.S.A.

“Security Implications of the Internet Protocol version 6”. BSDCan 2010, May 13-14, 2010, Ottawa, ON, Canada.

“Introducción a la Internet Engineering Task Force (IETF)”. INET 2010. Montevideo, Julio 2, 2010, Uruguay.

“An Overview of IPv6 Transition/Co-existence Technologies”. LACNOG 2010, October 19-22, 2010. Sao Paulo, Brazil.

“Results of a Security Assessment of the Internet Protocol version 6 (IPv6)”. LACNOG 2010, October 19-22, 2010. Sao Paulo, Brazil.

“Moving the Endpoint Identifier (EID) Option to Obsolete Status”. 79th IETF Meeting, November 7-12, 2010. Beijing, China.

“Security Assessment of the IPv6 Flow Label”. 79th IETF Meeting, November 7-12, 2010. Beijing, China.

“Mitigating Teredo Routing Loop Attacks”. 79th IETF Meeting, November 7-12, 2010. Beijing, China.

“Deprecation of ICMP Source Quench messages”. 79th IETF Meeting, November 7-12, 2010. Beijing, China.

“Results of a Security Assessment of the Internet Protocol (IP)”. UK CPNI offices, April 23, 2009. London, United Kingdom.

“Results of a Security Assessment of the Transmission Control Protocol (TCP)”. UK CPNI offices, April 23, 2009. London, United Kingdom.

“IPv6 deployment issues”. UK CPNI offices, April 24, 2009. London, United Kingdom.

“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.

“Results of a Security Assessment of the IETF Specifications of the TCP and IP Protocols”, Tercer Evento de Securidad en Redes (LACNIC XI), May 26-30, 2008. Salvador de Bahía, Brasil.

“Resultados de un análisis de seguridad de los protocolos TCP/IP”, Congreso Internacional de Ingeniería en Computación, September 23-26, 2008. Ixtlahuaca, México.

“Servicios de directorio de Internet”, Congreso Internacional de Ingeniería en Computación, September 23- 26, 2008, Ixtlahuaca, México.

“Redes móviles”, foro realizado en el marco del Congreso Internacional de Ingeniería en Computación, September 23-26, 2008. Ixtlahuaca, México.

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

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

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

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

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

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

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

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

“Security implications of Network Address Translators (NATs)”, 73rd IETF Meeting, November 16-21, 2008. Minneapolis, MN, USA.

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

“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 30 and December 1, 2007. Buenos Aires, Argentina.

“Ataques ICMP contra TCP” (videoconferencia), June 6th, 2006, Buenos Aires, Argentina, sponsored by the Argentinian Section of the IEEE, The Argentinian Chapter of the IEEE Computer Society, and RETINA. (http://vc.ieee.org.ar/abstract-vc-gont-retina-06-06.txt)

“Ataques ICMP contra TCP”, June 8th, 2006, Buenos Aires, Argentina, sponsored by the Argentinian Chapter of the IEEE Computer Society. (http://www.ieee.org.ar/noticiasdetalle.asp?IDNoticia=143)

“Reacción de TCP a errores ICMP”, Primeras Jornadas de Divulgación Electrónica de UTN/FRH. October 23-26, 2006, Buenos Aires, Argentina.

“Ataques de reseteo de conexión contra TCP”, Primeras Jornadas de Divulgación Electrónica de UTN/FRH. October 23-26, 2006, Buenos Aires, Argentina.

“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.

“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, Finlandia.

“Hackeando TCP”, Ciclo de charlas abiertas, UTN/FRH, August 2005, Buenos Aires, Argentina.

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

“Ataques ICMP contra TCP”, CaFeConf 2005 (4tas Jornadas de Software Libre y GNU/Linux), October 2005, Buenos Aires, Argentina.

“Solucionando la vulnerabilidad del mecanismo Path-MTU Discovery”, CaFeConf 2005 (4tas Jornadas de Software Libre y GNU/Linux), October 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.