

Fernando Gont

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

Mobile phone: (+54 9) 11 6536 4380

Web site: <http://www.gont.com.ar>

PGP Fingerprint: 7809 84F5 322E 45C7 F1C9 3945 96EE A9EF D076 FFF1

Publications

Technical Reports:

- ◆ 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:

- ◆ 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:

- ◆ Gont, F., “Recommendations for IPv6 Firewall Design and Implementation”, IETF Internet Draft, January 2012. (available on request).
- ◆ Gont, F., “Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard)”, IETF Internet Draft, January 2012. Available at: <http://www.ietf.org/internet-drafts/draft-gont-v6ops-ra-guard-implementation-00.txt>
- ◆ Gont, F., “Security Implications of the Use of IPv6 Extension Headers with IPv6 Neighbor Discovery”, IETF Internet Draft, January 2012. Available at: <http://www.ietf.org/internet-drafts/draft-gont-6man-nd-extension-headers-02.txt>

- ◆ 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, December 2011. Available at: <http://www.ietf.org/internet-drafts/draft-gont-6man-predictable-fragment-id-00.txt>
- ◆ Gont, F., “Processing of IPv6 "atomic" fragments”, IETF Internet Draft, December 2011. Available at: <http://www.ietf.org/internet-drafts/draft-gont-6man-ipv6-atomic-fragments-00.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., “A method for Generating Stable Privacy-Enhanced Addresses with IPv6 Stateless Address Autoconfiguration (SLAAC)”, IETF Internet Draft, December 2011. Available at: <http://www.ietf.org/internet-drafts/draft-gont-6man-stable-privacy-addresses-00.txt>
- ◆ Gont, F., Bellovin, S., “Defending Against Sequence Number Attacks”, IETF Internet Draft, December 2011. 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/id/draft-ietf-tcpm-rfc1948bis-02.txt>
- ◆ Gont, F., “Deprecation of ICMP Source Quench messages”, IETF Internet Draft, December 2011. This document has been accepted as a working group item of the TSV WG (<http://datatracker.ietf.org/wg/tsvwg/charter/>). Available at: <http://www.ietf.org/internet-drafts/draft-ietf-tsvwg-source-quench-03.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., “Security Implications of Predictable Fragment Identification Values”, IETF Internet Draft, December 2011. Available at: <http://www.ietf.org/internet-drafts/draft-gont-6man-predictable-fragment-id-00.txt>
- ◆ Gont, F., “Processing of IPv6 'atomic' fragments”, IETF Internet Draft, December 2011. Available at: <http://www.ietf.org/internet-drafts/draft-gont-6man-ipv6-atomic-fragments-00.txt>
- ◆ Gont, F., Atkinson, R., “IP Options Filtering Recommendations”, IETF Internet Draft, December 2011. Available at: <http://www.ietf.org/internet-drafts/draft-gont-opsec-ip-options-filtering-02.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., “Security Implications of the Use of IPv6 Extension Headers with IPv6 Neighbor Discovery”, IETF Internet Draft, June 2011. Available at: <http://tools.ietf.org/id/draft-gont-6man-nd-extension-headers-01.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. 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-02.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 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., “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., 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**, October 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, Poland. 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 efimeros”, **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., “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>

Presentations

- ◆ “ICMP attacks”, **CanSecWest 2005 Conference**, May 2005, Vancouver, **Canadá**.
- ◆ “ICMP attacks against TCP”, **BSDCan 2005 Conference**, May 2005, Ottawa, **Canadá**.
- ◆ “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, **Canadá**.
- ◆ “TCP’s reaction to soft errors”, **64th IETF Meeting**, November 6-11, 2005, Vancouver, BC, **Canadá**.
- ◆ “TCP User Timeout Option”, **64th IETF Meeting**, November 6-11, 2005, Vancouver, BC, **Canadá**.
- ◆ “Ataques ICMP contra TCP” (videoconferencia), June 6th, 2005, 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.**
- ◆ “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, **Perú**.
- ◆ “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, **Perú**.
- ◆ “Mejorando la seguridad de TCP/IP mediante aleatorización de parámetros de protocolo”, **ekoparty security conference**, November 30 and December 1, 2007. Buenos Aires, **Argentina**.
- ◆ “Results of a Security Assessment of the IETF Specifications of the TCP and IP Protocols”, **Tercer Evento de Seguridad en Redes (LACNIC XI)**, May 26-30, 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**.
- ◆ “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**.
- ◆ “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**.
- ◆ “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 – Edición N°2**, December 14, 2011. Buenos Aires, **Argentina**.

Participation in Program Committees

- ◆ **IEEE 18th International Conference on Computer Communications and Networks (ICCCN 2009)**, Track on Network Architecture and Protocols (NAP). Available at: <http://icccn.org/icccn09/tracks/nap.html>
- ◆ **Cuarto Evento de Seguridad en Redes de América Latina y el Caribe** (in the context of LACNIC XIII). May 24-29, 2009, Ciudad de Panamá, Panamá.
- ◆ **LACSEC 2010 - 5to Evento de Seguridad en Redes para América Latina y el Caribe** (in the context of LACNIC XIV). May 18-21, 2010, Curacao, Antillas Neerlandesas.
- ◆ **LACSEC 2011 - 6to Evento de Seguridad en Redes para América Latina y el Caribe** (in the context of LACNIC XV). May 15-20, 2011, Cancún, Mexico. **Chair** of the Program Committee.
- ◆ **LACSEC 2012 - 7mo Evento de Seguridad en Redes para América Latina y el Caribe** (in the context of LACNIC XVII). (to take place in) May 2012, Quito, Ecuador. **Chair** of the Program Committee.

Collaboration in third-party publications

IETF RFCs:

As part of my participation in the IETF (Internet Engineering Task Force), I have collaborated with the authors of a number of RFCs, and have thus received the corresponding credit in the “Acknowledgements” section of the aforementioned documents.

- ◆ Bashyam, M., Jethanandani, M., Ramaiah, A., “TCP Sender Clarification for Persist Condition”, IETF **RFC 6429**. December 2011. Available at: <http://tools.ietf.org/rfc/rfc6429.txt>
- ◆ Amante, S., Carpenter, B., Jiang, S., Rahajalme, J., “IPv6 Flow Label Specification”, IETF **RFC 6437**. November 2011. Available at: <http://tools.ietf.org/rfc/rfc6437.txt>
- ◆ Amante, S., Carpenter, B., Jiang, S., “Rationale for Update to the IPv6 Flow Label Specification”, IETF **RFC 6436**. November 2011. Available at: <http://tools.ietf.org/rfc/rfc6436.txt>
- ◆ van Beijnum, I., “An FTP Application Layer Gateway (ALG) for IPv6-to-IPv4 Translation”, IETF **RFC 6384**. October 2011. Available at: <http://tools.ietf.org/rfc/rfc6384.txt>
- ◆ Krishnan, S., Thaler, D., Hoagland, J., “Security Concerns With IP Tunneling”, IETF **RFC 6169**. April 2011. Available at: <http://tools.ietf.org/rfc/rfc6169.txt>
- ◆ Simpson, W.A., “TCP Cookie Transactions (TCPCT)”, IETF **RFC 6013**. January 2011. Available at: <http://tools.ietf.org/rfc/rfc6013.txt>
- ◆ Ramaiah, A., Stewart, R., Dalal, M., “Improving TCP’s Robustness to Blind In-Window Attacks”, IETF **RFC 5961**. August 2010. Available at: <http://tools.ietf.org/rfc/rfc5961.txt>
- ◆ Gagliano, R., “IPv6 Deployment in Internet Exchange Points (IXPs)”, IETF **RFC 5963**. August 2010. Available at: <http://tools.ietf.org/rfc/rfc5508.txt>
- ◆ Srisuresh, P., Ford, B., Sivakumar, S., Guha, S “NAT Behavioral Requirements for ICMP protocol”, IETF **RFC 5508**. April 2009. Available at: <http://tools.ietf.org/rfc/rfc5508.txt>
- ◆ Fairhurst, G., “The Datagram Congestion Control Protocol (DCCP) Service Codes”, IETF **RFC 5595**. September 2009. Available at: <http://tools.ietf.org/rfc/rfc5595.txt>
- ◆ Kao, M., “Current Operational Security Practices in Internet Service Provider Environments”, IETF **RFC 4778**. January 2007. Available at: <http://tools.ietf.org/rfc/rfc4778.txt>
- ◆ Guha, S., Biswas, K., Ford, B., Sivakumar, S., Srisuresh, P., “NAT Behavioral Requirements for TCP”, IETF **RFC 5382**. October 2008. Available at: <http://tools.ietf.org/rfc/rfc5382.txt>
- ◆ Bonica, R., Gan, D., Nikander, P., Tappan, D., Pignataro, C., “Extended ICMP to Support Multi-Part Messages”, IETF **RFC 4884**. April 2007. Available at: <http://tools.ietf.org/rfc/rfc4884.txt>

- ◆ Touch, J., “Defending TCP Against Spoofing Attacks”, IETF **RFC 4953**. July 2007. Available at: <http://tools.ietf.org/rfc/rfc4953.txt>
- ◆ Eddy, W., “TCP SYN Flooding Attacks and Common Mitigations”, IETF **RFC 4987**. August 2007. Available at: <http://tools.ietf.org/rfc/rfc4953.txt>

IETF Internet-Drafts:

As part of my participation in the IETF (Internet Engineering Task Force), I have collaborated with the authors of a number of Internet-Drafts, and have thus received the corresponding credit in the “Acknowledgements” section of the aforementioned documents.

- ◆ Baker, F., “Testing Eyeball Happiness”, IETF Internet Draft (draft-baker-bmwg-testing-eyeball-happiness-01.txt). December 2010. Available at: <http://tools.ietf.org/id/draft-baker-bmwg-testing-eyeball-happiness-01.txt>
- ◆ Roy, S., Durand, A., y Paugh, J., “Issues with Dual Stack IPv6 on by Default”, IETF Internet-Draft (draft-ietf-v6ops-v6onbydefault-02.txt). July 2004. Available at: <http://tools.ietf.org/id/draft-ietf-v6ops-v6onbydefault-03.txt>
- ◆ Sarolahti, P., Floyd, S., Kojo, M. “Transport-layer Considerations for Explicit Cross-layer Indications”, IETF Internet Draft (draft-sarolahti-tsvwg-crosslayer-01.txt). September 2007. Available at: <http://tools.ietf.org/id/draft-sarolahti-tsvwg-crosslayer-01.txt>

Technical Reports:

- ◆ Frankel, S., Graveman, R., Pearce, J., Rooks, M. “Guidelines for the Secure Deployment of IPv6”. Recommendations of the **National Institute of Standards and Technology**. Special Publication 800-119. December 2010. Disponible en: <http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf>. I reviewed the aforementioned report, and thus received the corresponding credit in the “Acknowledgments” section of the document.

Books:

- ◆ I performed a technical review of three chapters about TCP/IP network programming of the book “**The Linux Programming Interface: A Linux and UNIX System Programming Handbook**” (<http://nostarch.com/tlpi>), authored by **Michael Kerrisk**. I received the corresponding credit in the preface of the book.
- ◆ I performed a technical review of the book “**The TCP/IP Guide**”, authored by **Charles M. Kozierek**, and received the corresponding credit in the preface of the book (http://www.tcpipguide.com/free/t_Acknowledgments.htm)
- ◆ I performed a technical review of the book “**Patterns in Network Architecture**”, authored by **John Day**. I I received the corresponding credit in the preface of the book.
- ◆ I wrote excercises and performed a technical review of the book “**Business Data Communications**” authored by **William Stallings**. I received the corresponding credit in the “Acknowledgements” section of the book.
- ◆ I wrote excercises for several chapters (“Traditional Applications”, “Modern Applications”, “Protocols for QoS Support”, “Exterior Routing Protocols and Multicast” and “Sockets Programming”) of the book “**Computer Networks with Internet Protocols and Technology**”, authored by **William Stallings**. I received the corresponding credit in the “Acknowledgements” section of the book. Additionally, I performed a technical review of the chapters “Protocols for QoS Support” and “Exterior Routing Protocols and Multicast”.
- ◆ I performed a technical review of the chapter “Transport Protocols” of the 7th edition of the book “**Data and Computer Communications**”, authored by **William Stallings**. I received the corresponding credit in the “Acknowledgements” section of the book (ftp://ftp.prenhall.com/pub/esm/sample_chapters/cs/stallings/pdf/preface.pdf).
- ◆ I wrote exercises and performed a technical review of all the chapaters of the book “**Operating Systems**”, authored by **William Stallings**. I received the corresponding credit in the “Acknowledgements” section of the book.
- ◆ I wrote exercises for all the chapters of the book “**Data and Computer Communications**”, authored by **William Stallings**. I received the corresponding credit in the “Acknowledgements” section of the book.

- ◆ I wrote exercises for all the chapters of the book “**Cryptography and Network Security**”, authored by **William Stallings**. I received the corresponding credit in the “Acknowledgements” section of the book.

Vulnerability advisories

My work in the area of communications protocols security has led to the publication of the following vulnerability advisories, which acknowledge my work:

- ◆ **RedHat Security Advisory RHSA-2011:1465-1**: Important: kernel security and bug fix update (<https://rhn.redhat.com/errata/RHSA-2011-1465.html>)
- ◆ USN-1253-1: Linux kernel vulnerabilities (<http://www.ubuntu.com/usn/usn-1253-1/>)
- ◆ **SUSE Security Announcement: Linux kernel security update** (SUSE-SA:2011:046) (<http://lists.opensuse.org/opensuse-security-announce/2011-12/msg00011.html>)
- ◆ **UK's NISCC**: NISCC Vulnerability Advisory ICMP - 532967 (*Vulnerability Issues in ICMP packets with TCP payloads*) (<http://www.niscc.gov.uk/niscc/docs/al-20050412-00308.html?lang=en>)
- ◆ **US-CERT**: TCP/IP implementations do not adequately validate ICMP error messages (<http://www.kb.cert.org/vuls/id/222750>)
- ◆ **Cisco Systems**: Crafted ICMP Messages Can Cause Denial of Service (http://www.cisco.com/en/US/products/products_security_advisory09186a0080436587.shtml)
- ◆ **Microsoft Corp.**: Microsoft Security Bulletin Summary for April 2005 (<http://www.microsoft.com/technet/security/bulletin/ms05-apr.mspx>)
- ◆ **Sun Microsystems**: Sun TCP Connections May Experience Performance Degradation If Certain ICMP Error Messages Are Received (<http://sunsolve.sun.com/search/document.do?assetkey=1-26-57746-1>)
- ◆ **SCO Group**: TCP Remote ICMP Denial Of Service Vulnerabilities (<ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2005.38/SCOSA-2005.38.txt>)

Press

My work in the area of communications protocols security has led to the publication of the following articles and interviews:

- ◆ **Golem.de**: Interview Fernando Gont zur Sicherheit in IPv6 (<http://video.golem.de/internet/6452/fernando-gont-interview-zur-sicherheit-in-ipv6.html>)
- ◆ **Computerworld Mexico**: Podcast: Seguridad en IPv6 (<http://www.computerworldmexico.mx/podcasts.aspx?id=45>)
- ◆ **TechTarget.com**: Lagging Security Features, Vulnerabilities Could Hamper Transition to New Internet (<http://searchsecurity.techtarget.com/news/2240036676/Lagging-IPv6-security-features-vulnerabilities-could-hamper-transition>)
- ◆ **TechTarget.com**: World IPv6 recap (<http://itknowledgeexchange.techtarget.com/wans/world-ipv6-day-recap/>)
- ◆ **Prensa LACNIC**: Fernando Gont - IPv6 - LACNOG 2011 (<http://www.youtube.com/watch?v=Ta1iwffcIA>)
- ◆ **SecurityFocus**: U.K. response team releases Net security guide (<http://www.securityfocus.com/brief/800>)
- ◆ **SC Magazine**: UK government blast TCP/IP security (<http://www.securecomputing.net.au/News/120418-uk-government-blast-tcpip-security.aspx>)
- ◆ **UK's National Infrastructure Security Co-ordination Centre**: NISCC - the Quarterly (01/06) (<http://www.niscc.gov.uk/docs/re-20060818-00564.pdf>)
- ◆ **CNET News**: Bug hunters, software firms in uneasy alliance (http://news.com.com/Bug+hunters+%2C+software+firms+in+uneasy+alliance/2100-1002_3-5846019.html)
- ◆ **SecurityFocus**: Big debate over small packets (<http://www.securityfocus.com/news/11306>)
- ◆ **KernelTrap**: OpenBSD Hackathon 2005, Part III (<http://kerneltrap.org/node/5382>)

- ◆ **ZDNet UK News:** *Microsoft silent over IP vulnerability claims*
(<http://news.zdnet.co.uk/internet/security/0,39020375,39195206,00.htm>)
- ◆ **SecurityFocus:** *OpenBSD's network stack* (<http://www.securityfocus.com/columnists/361>)
- ◆ **Golem.de:** *ICMP kann TCP/IP Probleme machen* (<http://www.golem.de/0504/37482.html>)
- ◆ **Tecchannel:** *ICMP-Nachrichten erlauben Angriffe auf TCP/IP*
(<http://www.tecchannel.de/news/themen/sicherheit/422835/>)