



## Fernando Gont

E-mail: [fernando@gont.com.ar](mailto:fernando@gont.com.ar)

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

E-mail: [fgont@si6networks.com](mailto:fgont@si6networks.com)

PGP Fingerprint: 6666 31C6 D484 63B2 8FB1 E3C4 AE25 0D55 1D4E 7492

Personal Web site: <https://www.gont.com.ar>

LinkedIn profile: <https://www.linkedin.com/in/fernandogont>

IETF profile: <https://datatracker.ietf.org/person/Fernando%20Gont>

Github profile: <https://github.com/fgont>

Google Scholar: <https://bit.ly/3xebq7g>

---

### Brief Biography

Fernando Gont is a Security Researcher and Consultant at SI6 Networks.

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.

He is active in several working groups of the Internet Engineering Task Force (IETF), where he has led many improvements to the IPv6 protocol suite, and has published 36 IETF RFCs (Request For Comments). Gont has also developed the SI6 Network's IPv6 Toolkit (<<https://www.si6networks.com/tools/ipv6toolkit>>) -- a free, portable and comprehensive security assessment toolkit for the IPv6 protocol suite.

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 2011, DEEPSEC 2011, Hackito Ergo Sum 2012, German IPv6 Kongress 2014, H2HC 2017, Positive Hack Days 8, Hack In Paris 2018, and Troopers 2018. Additionally, he is a regular attendee of the Internet Engineering Task Force (IETF) meetings.

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

## Publications

### Technical Reports:

- ◆ Gont, F., “DNS Privacy Frequently Asked Questions (FAQ)”. Written on behalf of the **Internet Society**. Available at: <https://www.internetsociety.org/resources/deploy360/dns-privacy/faq/>
- ◆ Gont, F., “IPv6 Security for IPv4 Engineers”. Written on behalf of the **Internet Society**. Available at: <https://www.internetsociety.org/resources/deploy360/ipv6/security/ipv4-engineers>
- ◆ Gont, F., “Introduction to DNS Privacy”. Written on behalf of the **Internet Society**. Available at: <https://www.internetsociety.org/resources/deploy360/dns-privacy/intro/>
- ◆ Gont, F., “IPv6 Security Frequently Asked Questions (FAQ)”. Written on behalf of the **Internet Society**. Available at: <https://www.internetsociety.org/deploy360/ipv6/faq/>
- ◆ 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:

- ◆ Gont, F., Hilliard, N., Doering, G., Kumari, W., Huston, G., Liu, W. “Operational Implications of IPv6 Packets with Extension Headers”, **IETF RFC 9098**. September 2021. Available at: <https://tools.ietf.org/pdf/rfc9098.pdf>
- ◆ Gont, F., Zorz, J., Patterson, R., “Improving the Reaction of Customer Edge Routers to Renumbering Events”. **IETF RFC 9096**. Available at: <https://tools.ietf.org/pdf/rfc9096.pdf>
- ◆ Gont, F., Gont, G., Lichvar, M., “Network Time Protocol Version 4: Port Randomization”, **IETF RFC 9109**. August 2021. Available at: <https://tools.ietf.org/pdf/rfc9109.pdf>
- ◆ Gont, F., Krishnan, S., Narten, T., Draves, R. “Temporary Address Extensions for Stateless Address Autoconfiguration in IPv6”, **IETF RFC 8981**. February 2021. Available at: <https://tools.ietf.org/pdf/rfc8981.pdf>
- ◆ Gont, F., Zorz, J., Patterson, R. “Reaction of Stateless Address Autoconfiguration (SLAAC) to Flash-Renumbering Events”, **IETF RFC 8978**. March 2021. Available at: <https://tools.ietf.org/pdf/rfc8978.pdf>
- ◆ Bonica, R., Baker, F., Huston, G., Hinden, R., Troan, O., Gont, F. “IP Fragmentation Considered Fragile”, **IETF RFC 8900**. September 2020. Available at: <https://tools.ietf.org/pdf/rfc8900>
- ◆ Gont, F., Cooper, A., Thaler, D., Liu, W. “Recommendation on Stable IPv6 Interface Identifiers”. **IETF RFC 8064**. February 2017. Available at: <https://www.rfc-editor.org/rfc/rfc8064.txt>
- ◆ Gont, F., Liu, W., Anderson, T., “Generation of IPv6 Atomic Fragments Considered Harmful”. **IETF RFC 8021**. January 2017. Available at: <https://www.rfc-editor.org/rfc/rfc8021.txt>

- ◆ Gont, F., Liu, W. “A Method for Generating Semantically Opaque Interface Identifiers with Dynamic Host Configuration Protocol for IPv6 (DHCPv6)”. **IETF RFC 7943**. Available at: <https://www.rfc-editor.org/rfc/rfc7943.txt>
- ◆ Bao, C., Li, X., Baker, F., Anderson, T., Gont, F. “IP/ICMP Translation Algorithm”, **IETF RFC 7915**. Available at: <https://www.rfc-editor.org/rfc/rfc7915.txt>
- ◆ Gont, F., Linkova, J., Chown, T., Liu, W. “Observations on the Dropping of Packets with IPv6 Extension Headers in the Real World”, **IETF RFC 7872**. Available at: <https://www.rfc-editor.org/rfc/rfc7872.txt>
- ◆ Gont, F., “Security Implications of Predictable Fragment Identification Values”. **IETF RFC 7739**. Available at: <https://www.rfc-editor.org/rfc/rfc7739.txt>.
- ◆ Cooper, A., Gont, F., Thaler, D. “Security and Privacy Considerations for IPv6 Address Generation Mechanisms”. **IETF RFC 7721**. Available at: <https://www.rfc-editor.org/rfc/rfc7721.txt>.
- ◆ Gont, F., Chown, T., “Network Reconnaissance in IPv6 Networks”. **IETF RFC 7707**. Available at: <https://www.rfc-editor.org/rfc/rfc7707.txt>.
- ◆ Gont, F., Liu, W., Van de Velde, G., “DHCPv6-Shield: Protecting Against Rogue DHCPv6 Servers”. **IETF RFC 7610**, August 2015. Available at: <https://www.rfc-editor.org/rfc/rfc7610.txt>
- ◆ Bagnulo, M., Paasch, C., Gont, F., Bonaventure, O., Raiciu, C. “Analysis of MPTCP residual threats and possible fixes”, **IETF RFC 7430**, July 2015. Available at: <https://www.rfc-editor.org/rfc/rfc7430.txt>
- ◆ Carpenter, B., Chown, T., Gont, F., Jiang, S., Petrescu, A., Yourtchenko, A. “Analysis of the 64-bit Boundary in IPv6 Addressing”, **IETF RFC 7421**, January 2015. Available at: <https://www.rfc-editor.org/rfc/rfc7421.txt>
- ◆ Gont, F., “Layer 3 Virtual Private Network (VPN) Tunnel Traffic Leakages in Dual-Stack Hosts/Networks”, **IETF RFC 7359**, August 2014. Available at: <https://www.rfc-editor.org/rfc/rfc7359.txt>
- ◆ Gont, F., “A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)”, **IETF RFC 7217**, April 2014. Available at: <http://www.rfc-editor.org/rfc/rfc7217.txt>
- ◆ Gont, F., Atkinson, R., Pignataro, C., “Recommendations on Filtering of IPv4 Packets Containing IPv4 Options”, **IETF RFC 7126**, February 2014. Available at: <https://www.rfc-editor.org/rfc/rfc7126.txt>
- ◆ Gont, F., “Security Implications of IPv6 on IPv4 Networks”, **IETF RFC 7123**, February 2014. Available at: <https://www.rfc-editor.org/rfc/rfc7123.txt>
- ◆ Gont, F., “Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard)”, **IETF RFC 7113**, February 2014. Available at: <https://www.rfc-editor.org/rfc/rfc7113.txt>
- ◆ Gont, F., Manral, V., Bonica, R. “Implications of Oversized IPv6 Header Chains”, **IETF RFC 7112**, January 2014. Available at: <https://www.rfc-editor.org/rfc/rfc7112.txt>
- ◆ Gont, F., “Security Implications of IPv6 Fragmentation with IPv6 Neighbor Discovery”, **IETF RFC 6980**, August 2013. Available at: <http://www.rfc-editor.org/rfc/rfc6980.txt>
- ◆ Gont, F. 'Processing of IPv6 "Atomic" Fragments'. **IETF RFC 6946**. May 2013. Available at: <https://www.rfc-editor.org/rfc/rfc6946.txt>
- ◆ Gont, F. “Formally Deprecating Some ICMPv4 Message Types”, **IETF RFC 6918**. April 2013. Available at: <https://www.rfc-editor.org/rfc/rfc6918.txt>
- ◆ Pignataro, C., Gont, F., “Formally Deprecating some IPv4 Options”, **IETF RFC 6814**. November 2012. Available at: <https://www.rfc-editor.org/rfc/rfc6814.txt>
- ◆ Gont, F. “Deprecation of ICMP Source Quench messages”, **IETF RFC 6633**. May 2012. Available at: <https://www.rfc-editor.org/rfc/rfc6633.txt>
- ◆ Gont, F., Bellovin, S., “Defending Against Sequence Number Attacks”, **IETF RFC 6528**. February 2012. Available at: <https://www.rfc-editor.org/rfc/rfc6528.txt>
- ◆ Gont, F. “Security Assessment of the Internet Protocol version 4”, **IETF RFC 6274**. July 2011. Available at: <https://www.rfc-editor.org/rfc/rfc6274.txt>
- ◆ Gont, F., “Reducing the TIME-WAIT state using TCP timestamps”, **IETF RFC 6191**. April 2011. Available at: <https://www.rfc-editor.org/rfc/rfc6191.txt>
- ◆ Larsen, M., Gont, F. “Transport Protocol Port Randomization Recommendations”, **IETF RFC 6056**. Available at: <https://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: <https://www.rfc-editor.org/rfc/rfc6093.txt>
- ◆ Gont, F., “ICMP attacks against TCP”, **IETF RFC 5927**. July 2010. Available at: <https://www.rfc-editor.org/rfc/rfc5927.txt>
- ◆ Eggert, L., Gont, F., “TCP User TimeOut (UTO) Option”, **IETF RFC 5482**. March 2009. Available at: <https://www.rfc-editor.org/rfc/rfc5489.txt>
- ◆ Gont, F., “TCP’s Reaction to Soft Errors”. **IETF RFC 5461**. February 2009. Available at: <https://www.rfc-editor.org/rfc/rfc5461.txt>

## **IETF Internet-Drafts:**

### **Working Group items**

- ◆ Gont, F., Zorz, J., Patterson, R., “Improving the Reaction of Stateless Address Autoconfiguration (SLAAC) to Renumbering Events”, IETF Internet-Draft. Available at: <https://tools.ietf.org/html/draft-ietf-6man-slaac-renum>
- ◆ Gont, F., Liu, W., Bonica, R. “Recommendations on Filtering of IPv6 Packets Containing IPv6 Extension Headers”, IETF Internet-Draft. Available at: <https://tools.ietf.org/html/draft-ietf-opsec-ipv6-eh-filtering>
- ◆ Gont, F., Bonica, R., Liu, W. “Validation of IPv6 Neighbor Discovery Options”, IETF Internet-Draft. Available at: <https://tools.ietf.org/html/draft-ietf-6man-nd-opt-validation>
- ◆ Gont, F. “Security Assessment of Neighbor Discovery (ND) for IPv6”. IETF Internet-Draft. 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-nd-security>

### **Individual submissions**

- ◆ Gont, F., Arce, I. “Security Considerations for Transient Numeric Identifiers Employed in Network Protocols”, IETF Internet-Draft. Available at: <https://tools.ietf.org/html/draft-gont-numeric-ids-sec-considerations>
- ◆ Gont, F., Huitema, C., Krishnan, S., Gont, G., Garcia Corbo, M. “Recommendation on Temporary IPv6 Interface Identifiers”, IETF Internet-Draft. Available at: <https://tools.ietf.org/html/draft-gont-6man-non-stable-iids>
- ◆ Bush, R., Carpenter, B., Gont, F., Hilliard, N., Jaeggli, J., Huston, G., Morrow, C., Snijders, J. “IPv6 is Classless”. Available at: <https://tools.ietf.org/html/draft-bourbaki-6man-classless-ipv6>
- ◆ Gont, F., Baker, F. “On Firewalls in Network Security”, IETF Internet-Draft. Available at: <https://tools.ietf.org/html/draft-gont-opsawg-firewalls-analysis>
- ◆ Gont, F., Hunter, R., Massar, J., Liu, W. “Network Ingress Filtering: Defeating Attacks which employ Forged ICMP/ICMPv6 Error Messages”, IETF Internet-Draft. Available at: <https://tools.ietf.org/html/draft-gont-opsec-icmp-ingress-filtering>
- ◆ Gont, F., Liu, W., Bonica, R. “Transmission and Processing of IPv6 Options”, IETF Internet-Draft. Available at: <https://tools.ietf.org/html/draft-gont-6man-ipv6-opt-transmit>
- ◆ Gont, F., Liu, W. “IPv6 Universal Extension Header”, IETF Internet-Draft. Available at: <http://tools.ietf.org/html/draft-gont-6man-ipv6-universal-extension-header>
- ◆ Gont, F., Borman, D. “On the Validation of TCP Sequence Numbers”. IETF Internet-Draft. Available at: <http://tools.ietf.org/html/draft-gont-tcpm-tcp-seq-validation>.
- ◆ 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://tools.ietf.org/html/draft-gont-intarea-obsolete-eid-option>
- ◆ Gont, F., “Processing of TCP segments with Mirrored End-points”, IETF Internet Draft, March 2012. Available at: <http://tools.ietf.org/html/draft-gont-tcpm-tcp-mirrored-endpoints>

- ◆ Gont, F., “Processing of IP Security/Compartment and Precedence Information by TCP”, IETF Internet Draft, March 2012. Available at: <http://tools.ietf.org/id/drafts/draft-gont-tcpm-tcp-seccomp-prec>.
- ◆ 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://tools.ietf.org/id/draft-gont-6man-flowlabel-security>.
- ◆ 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>
- ◆ 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>
- ◆ 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>
- ◆ 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>

## **IRTF Internet-Drafts:**

### **Research Group items**

- ◆ Gont, F., Arce, I. “Unfortunate History of Transient Numeric Identifiers”, IRTF Internet-Draft. Available at: <https://tools.ietf.org/id/draft-irtf-pearg-numeric-ids-history>
- ◆ Gont, F., Arce, I. “On the Generation of Transient Numeric Identifiers”, IRTF Internet-Draft. Available at: <https://tools.ietf.org/id/draft-irtf-pearg-numeric-ids-generation>

## 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.

## Web portal articles:

- ◆ Gont, F. “Understanding why IPv6 renumbering problems occur”. **TechTarget's SearchNetworking.Techtarget.com** Portal, September 2019. Available at: <<https://searchnetworking.techtarget.com/tip/Understanding-why-IPv6-renumbering-problems-occur>>.
- ◆ Gont, F., “How IPv6 SLAAC Responds to Renumbering Events”. **Internet Society’s Deploy360 Program**. February 2019. Available at: <https://www.internetsociety.org/blog/2019/02/slaac-renum-reaction>
- ◆ Gont, F. “The evolution of the Let’s Encrypt certificate authority”. **TechTarget's SearchSecurity.Techtarget.com** Portal, January 2019. Available at: <<https://searchsecurity.techtarget.com/tip/The-evolution-of-the-Lets-Encrypt-certificate-authority>>.
- ◆ Gont, F., “DNS-over-TLS in Linux (systemd)”. **Internet Society’s Deploy360 Program**. December 2018. Available at: <<https://www.internetsociety.org/blog/2018/12/dns-privacy-in-linux-systemd/>>
- ◆ Gont, F., “DNS-over-HTTPS (DoH) Support in Mozilla Firefox”. **Internet Society’s Deploy360 Program**. December 2018. Available at: <<https://www.internetsociety.org/blog/2018/12/dns-privacy-support-in-mozilla-firefox/>>
- ◆ Gont, F. “Ensuring P2P apps don't cause network performance issues with IPv6”. **TechTarget's SearchNetworking.Techtarget.com** Portal, August 2018. Available at: <<https://searchnetworking.techtarget.com/tip/Ensuring-P2P-apps-dont-cause-network-performance-issues-with-IPv6>>.
- ◆ Gont, F. “Network reconnaissance: How to use SI6 Networks' IPv6 toolkit”. **TechTarget's SearchSecurity.Techtarget.com** Portal, August 2018. Available at: <<https://searchsecurity.techtarget.com/tip/Network-reconnaissance-How-to-use-SI6-Networks-IPv6-toolkit>>.
- ◆ Gont, F. “What IPv6 features can be found in the latest specification?”. **TechTarget's SearchNetworking.Techtarget.com** Portal, August 2018. Available at: <<https://searchnetworking.techtarget.com/tip/What-IPv6-features-can-be-found-in-the-latest-specification>>.
- ◆ Gont, F. “What to do when IPv4 and IPv6 policies disagree”. **TechTarget's SearchSecurity.Techtarget.com** Portal, August 2018. Available at: <<https://searchsecurity.techtarget.com/tip/What-to-do-when-IPV4-and-IPv6-policies-disagree>>.
- ◆ Gont, F. “How hackers use idle scans in port scan attacks”. **TechTarget's SearchNetworking.Techtarget.com** Portal, August 2018. Available at: <<https://searchnetworking.techtarget.com/tip/How-hackers-use-idle-scans-in-port-scan-attacks>>.
- ◆ Gont, F. “Why IPv6 networks create DNS configuration problems”. **TechTarget's SearchNetworking.Techtarget.com** Portal, February 2018. Available at: <<http://searchnetworking.techtarget.com/tip/Why-IPv6-networks-create-DNS-configuration-problems>>.
- ◆ Gont, F. “How IPv6 deployment affects the security of IoT devices”. **TechTarget's InternetOfThingsAgenda.Techtarget.com** Portal. October 2017. Available at: <<http://internetofthingsagenda.techtarget.com/feature/How-IPv6-deployment-affects-the-security-of-IoT-devices>>.

- ◆ Gont, F. “IPv6 addresses: Stability concerns and usage advice”. **TechTarget's SearchSecurity.Techtarget.com** Portal, August 2017. Available at: <<http://searchsecurity.techtarget.com/tip/IPv6-addresses-Stability-concerns-and-usage-advice>>
- ◆ Gont, F. “IPv6 addresses: Security recommendations for usage”. **TechTarget's SearchSecurity.Techtarget.com** Portal, July 2017. Available at: <<http://searchsecurity.techtarget.com/tip/IPv6-addresses-Security-recommendations-for-usage>>
- ◆ Gont, F. “How to use an interface identifier to check for IPv6 network updates”. **TechTarget's SearchSecurity.Techtarget.com** Portal, June 2017. Available at: <<http://searchsecurity.techtarget.com/tip/How-to-use-an-interface-identifier-to-check-for-IPv6-network-updates>>
- ◆ Gont, F. “IPv6 update: A look at the security and privacy improvements”. **TechTarget's SearchSecurity.Techtarget.com** Portal, June 2017. Available at: <<http://searchsecurity.techtarget.com/tip/IPv6-update-A-look-at-the-security-and-privacy-improvements>>
- ◆ Gont, F. “Using IPv6 atomic fragments for a denial-of-service attack”. **TechTarget's SearchSecurity.Techtarget.com** Portal, March 2017. Available at: <<http://searchsecurity.techtarget.com/tip/Using-IPv6-atomic-fragments-for-a-denial-of-service-attack>>
- ◆ Gont, F. “How a single ICMPv6 packet can cause a denial-of-service attack”. **TechTarget's SearchSecurity.Techtarget.com** Portal, March 2017. Available at: <<http://searchsecurity.techtarget.com/tip/How-a-single-ICMPv6-packet-can-cause-a-denial-of-service-attack>>
- ◆ Gont, F. “How to leverage UDP port scanning as a security scanning tool”. **TechTarget's SearchNetworking.Techtarget.com** Portal, February 2017. Available at: <<http://searchnetworking.techtarget.com/tip/How-to-leverage-UDP-port-scanning-as-a-security-scanning-tool>>
- ◆ Gont, F. “DNS reverse address mapping: Exploiting the scanning technique”. **TechTarget's SearchSecurity.Techtarget.com** Portal, February 2017. Available at: <<http://searchsecurity.techtarget.com/tip/DNS-reverse-address-mapping-Exploiting-the-scanning-technique>>
- ◆ Gont, F. “How to use DNS reverse mapping to scan IPv6 addresses”. **TechTarget's SearchSecurity.Techtarget.com** Portal, February 2017. Available at: <<http://searchsecurity.techtarget.com/tip/How-to-use-DNS-reverse-mapping-to-scan-IPv6-addresses>>
- ◆ Gont, F. “Tips to understand different TCP port-scanning techniques”. **TechTarget's SearchNetworking.Techtarget.com** Portal, November 2016. Available at: <<http://searchnetworking.techtarget.com/tip/Tips-to-understand-different-TCP-port-scanning-techniques>>
- ◆ Gont, F. “MAC address randomization schemes: Examining the pros and cons”. **TechTarget's SearchSecurity.Techtarget.com** Portal, November 2016. Available at: <<http://searchsecurity.techtarget.com/tip/MAC-address-randomization-schemes-Examining-the-pros-and-cons>>
- ◆ Gont, F. “MAC address randomization: Understanding the security benefits”. **TechTarget's SearchSecurity.Techtarget.com** Portal, October 2016. Available at: <<http://searchsecurity.techtarget.com/tip/MAC-address-randomization-Understanding-the-security-benefits>>
- ◆ Gont, F. “Filtering IPv6 extension headers is sometimes necessary”. **TechTarget's SearchNetworking.Techtarget.com** Portal, November 2015. Available at: <<http://searchnetworking.techtarget.com/tip/Filtering-IPv6-extension-headers-is-sometimes-necessary>>
- ◆ Gont, F. “IPv6 filtering threatens impact of new protocol”. **TechTarget's SearchNetworking.Techtarget.com** Portal, September 2015. Available at: <<http://searchnetworking.techtarget.com/tip/IPv6-filtering-threatens-impact-of-new-protocol>>
- ◆ Gont, F. “How to perform IPv6 network reconnaissance”. **TechTarget's SearchSecurity.Techtarget.com** Portal, July 2015. Available at: <<http://searchsecurity.techtarget.com/tip/How-to-perform-IPv6-network-reconnaissance>>
- ◆ Gont, F. “How to evaluate IPv6 network security with SI6 Networks IPv6 Toolkit”. **TechTarget's SearchSecurity.Techtarget.com** Portal, February 2015. Available at: <<http://searchsecurity.techtarget.com/tip/How-to-evaluate-IPv6-network-security-with-SI6-Networks-IPv6-Toolkit>>

- ◆ Gont, F. “IPv6 attack attempts and how to mitigate them”. **TechTarget's SearchNetworking.Techtarget.com** Portal, February 2015. Available at: <<http://searchnetworking.techtarget.com/tip/IPv6-attack-attempts-and-how-to-mitigate-them>>
- ◆ Gont, F. “Mitigating IPv6 neighbor discovery attacks”. **TechTarget's SearchNetworking.Techtarget.com** Portal, February 2015. Available at: <<http://searchnetworking.techtarget.com/tip/Mitigating-IPv6-neighbor-discovery-attacks>>
- ◆ Gont, F. “How to protect your IPv6 address management”. **TechTarget's SearchNetworking.Techtarget.com** Portal, January 2015. Available at: <<http://searchnetworking.techtarget.com/tip/How-to-protect-your-IPv6-address-management>>
- ◆ Gont, F. “How to avoid IPv6 neighbor discovery threats”. **TechTarget's SearchNetworking.Techtarget.com** Portal, January 2015. Available at: <<http://searchnetworking.techtarget.com/tip/How-to-avoid-IPv6-neighbor-discovery-threats>>
- ◆ Gont, F. “IPv6 extension headers and security: Analyzing the risk”. **TechTarget's SearchSecurity.Techtarget.com** Portal, December 2014. Available at: <<http://searchsecurity.techtarget.com/tip/IPv6-extension-headers-and-security-Analyzing-the-risk>>
- ◆ Gont, F. “Understanding security flaws in IPv6 addressing schemes”. **TechTarget's SearchSecurity.Techtarget.com** Portal, December 2014. Available at: <<http://searchsecurity.techtarget.com/tip/Understanding-security-flaws-in-IPv6-addressing-schemes>>
- ◆ Gont, F. “IPv6 addressing requires special attention to ensure security”. **TechTarget's SearchNetworking.Techtarget.com** Portal, June 2013. Available at: <<http://searchnetworking.techtarget.com/tip/IPv6-addressing-requires-special-attention-to-ensure-security>>
- ◆ Gont, F. “Address IPv6 security before your time runs out”, **TechTarget's SearchSecurity.com** Portal. April 2013. Available at: <<http://searchsecurity.techtarget.com/feature/Address-IPv6-security-before-your-time-runs-out>>.
- ◆ Gont, F. “How to avoid security issues with VPN leaks on dual-stack networks”, **TechTarget's SearchSecurity.com** Portal. January 2013. Available at: <<http://searchsecurity.techtarget.com/tip/How-to-avoid-security-issues-with-VPN-leaks-on-dual-stack-networks>>.
- ◆ 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>



## Magazine Articles:

- ◆ 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., “Rastreado 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.

## Conference presentations

**Note:** All the slides for my presentations are available at: <<https://www.gont.com.ar/presentations>> and <<https://www.signetworks.com/presentations>>

- ◆ “Panel Discussion on IPv6 Extension Headers”. **Connections 2022**, April 7-8, 2022. Online event. [[video](#)]
- ◆ “Reconocimiento de redes IPv6”. **Ekoparty Hackademy** masterclass, March 17, 2022. Online event.
- ◆ “Improving the Reaction of IPv6 SLAAC to Renumbering Events”. **PLNOG 2022**, March 8-9, 2022. Online event.
- ◆ “Implicancias de Seguridad y Privacidad del Direcccionamiento IPv6”, **Security Day 2022**. January 29, 2022. Online event.
- ◆ “Update on IETF publications”. **UK IPv6 Council Annual Meeting**, December 7, 2021. Online event.

- ◆ “State of the Art in IPv6 Security”. **THE H@CK SUMMIT**, November 5, 2021. Online event.
- ◆ “Improving the Reaction of Customer Edge Routers to IPv6 Renumbering Events”. **NANOG 83**, November 1-3, 2021, Minneapolis, **U.S.A.**
- ◆ “Operational Implications of IPv6 Packets with Extension Headers”. **NANOG 83**, November 1-3, 2021, Minneapolis, **U.S.A.**
- ◆ “Operational Implications of IPv6 Packets with Extension Headers”. **LACNIC 36**, October 11-15, 2021. Online event.
- ◆ “Improving the Reaction of Customer Edge Routers to IPv6 Renumbering Events”. **LACNIC 36**, October 11-15, 2021. Online event.
- ◆ “IPv6 Extension Headers in the Real World”. **LACNIC 35**, May 12-14, 2021. Online event.
- ◆ “RFC 8981: Temporary Address Extensions for IPv6 SLAAC”. **LACNIC 35**, May 12-14, 2021. Online event.
- ◆ “Port Randomization in the Network Time Protocol Version 4”. **IETF 105**, NTP WG. July 20-26, 2019. Montreal, **Canada**.
- ◆ “Security and Privacy Implications of Numeric Identifiers Employed in Network Protocols”. **IETF 105**, PEARG. July 20-26, 2019. Montreal, **Canada**.
- ◆ “Hacking IPv6 Networks v5.0” (training course). Hack In Paris 2019. June 16-18, 2019. Paris, **France**.
- ◆ “Privacidad en el DNS”. **LACNIC 31**. May 6-10, 2019. Punta Cana, **Dominican Republic**.
- ◆ “SLAAC’s Reaction to Renumbering Events”. IETF 104, 6man Working Group. March 23-29, 2019. Prague, **Czech Republic**.
- ◆ “Security and Privacy Implications of Numeric Identifiers Employed in Network Protocols”. **IETF 104**. March 23-29, 2019. Prague, **Czech Republic**.
- ◆ “SLAAC’s Reaction to Renumbering Events”. **IETF 104**, v6ops Working Group. March 23-29, 2019. Prague, **Czech Republic**.
- ◆ “Privacy Extensions for Stateless Address Autoconfiguration in IPv6”. **IETF 104**. March 23-29, 2019. Prague, **Czech Republic**.
- ◆ “What are the IPv6 news from the IETF?”. **NGI @ Troopers 2019** . March 18-19, 2019. Heidelberg, **Germany**.
- ◆ “SI6 Toolkit v3.0”. **NGI @ Troopers 2019** . March 18-19, 2019. Heidelberg, **Germany**.
- ◆ “Network Reconnaissance in IPv6” (training course). **Security Day 2018**. December 2018. Guayaquil, **Ecuador**.
- ◆ “Despliegue de Redes IPv6 Seguras” (training course). **Claro Ecuador**. December 2018. Guayaquil, **Ecuador**.
- ◆ “Hacking IPv6 Networks v5.0” (training course). **Hack In Paris 2018**. June 25-29, 2018. Paris, **France**.
- ◆ “Knockin' on IPv6 Doors”. **Hack In Paris 2018**. June 25-29, 2018. Paris, **France**.
- ◆ “IPv6 Security: How did we get here?”. **PHDays 2018**. May 15-16, 2018. Moscow, **Russian Federation**.
- ◆ “Advances in IPv6 Network Reconnaissance”. **x33fcon 2018**. May 7-8, 2018. Gdynia, **Poland**.
- ◆ “Estado de Despliegue de IPv6 en Servicios de Internet para la Región de Latinoamérica y Caribe (LAC)”. **LACNIC 29**. Abril 30 - Mayo 4, 2018. Ciudad de Panamá, **Panama**.
- ◆ “Advances in IPv6 Network Reconnaissance”. **LACNIC 29**. Abril 30 - Mayo 4, 2018. Ciudad de Panamá, **Panama**.
- ◆ “Advances in IPv6 Network Reconnaissance ”. **NGI @ Troopers 2018** . March 12-13, 2018. Heidelberg, **Germany**.
- ◆ “Knockin' on IPv6 Doors ”. **NGI @ Troopers 2018** . March 12-13, 2018. Heidelberg, **Germany**.
- ◆ “Knockin' on IPv6 Doors”. **Hack In Paris 2018**. June 25-29, 2018. Paris, **France**.
- ◆ “IPv6 Security: How did we get here?”. **PHDays 2018**. May 15-16, 2018. Moscow, **Russian Federation**.

- ◆ “Advances in IPv6 Network Reconnaissance”. **x33fcon 2018**. May 7-8, 2018. Gdynia, **Poland**.
- ◆ “Estado de Despliegue de IPv6 en Servicios de Internet para la Región de Latinoamérica y Caribe (LAC)”. **LACNIC 29**. Abril 30 - Mayo 4, 2018. Ciudad de Panamá, **Panama**.
- ◆ “Advances in IPv6 Network Reconnaissance”. **LACNIC 29**. Abril 30 - Mayo 4, 2018. Ciudad de Panamá, **Panama**.
- ◆ “Advances in IPv6 Network Reconnaissance ”. **NGI @ Troopers 2018** . March 12-13, 2018. Heidelberg, **Germany**.
- ◆ “Knockin' on IPv6 Doors ”. **NGI @ Troopers 2018** . March 12-13, 2018. Heidelberg, **Germany**.
- ◆ “Hacking Smart Home Devices”. **H2HC 2017**. October 21-22, 2017. Sao Paulo, **Brazil**.
- ◆ “How IPv6 may affect IoT Security”. **FIRST TC**. September 18, 2017. Montevideo, **Uruguay**.
- ◆ “Network Reconnaissance in IPv6”. **PHDays VII**. May 23-24, 2017. Moscow, **Russia**.
- ◆ “IPv6 Security Tools”. **UK IPv6 Council Security Workshop**. July 12, 2017. London, **United Kingdom**.
- ◆ “Recent IPv6 Security Standardization Efforts”. **UK IPv6 Council Security Workshop**. July 12, 2017. London, **United Kingdom**.
- ◆ “State of the Art in IPv6 Attack & Defense”. **Africa Internet Summit 2017**. May 21 - June 2, 2017. Nairobi, **Kenya**.
- ◆ “Advanced IPv6 Network Reconnaissance”. **Africa Internet Summit 2017**. May 21 - June 2, 2017. Nairobi, **Kenya**.
- ◆ “IPv6 Security Workshop”. **Africa Internet Summit 2017**. May 21 - June 2, 2017. Nairobi, **Kenya**.
- ◆ “Hacking TP-Link Devices”. **NGI @ Troopers 17**. March 20-24, 2017. Heidelberg, **Germany**.
- ◆ “IPv6: Motivación, mitos, y desafíos”. **ITEC**. September 6, 2016. Rio Cuarto, Córdoba, **Argentina**.
- ◆ “Introducción y Experiencias en el IETF”. **ITEC**. September 6, 2016. Rio Cuarto, Córdoba, **Argentina**.
- ◆ “Seguridad IPv6”. **Universidad Nacional de Rio Cuarto (UNRC)**. August 25, 2016. Rio Cuarto, Córdoba, **Argentina**.
- ◆ “Introducción y Experiencias en el IETF”. **Universidad Nacional de Rio Cuarto (UNRC)**. August 25, 2016. Rio Cuarto, Córdoba, **Argentina**.
- ◆ “Seguridad y Privacidad en Direccionamiento IPv6”. **#1HackParaLosChicos 2016**. August 26, 2016. Córdoba, **Argentina**.
- ◆ “Advanced IPv6 Security” (training course). June 20, 23, and 24, 2016. Ljubljana, **Slovenia**.
- ◆ “Hacking IPv6 Networks -- with Hands-on Lab” (training course). **IPv6 Business Conference**. June 17, 2016. Zürich, **Switzerland**.
- ◆ “Hacking IPv6 Networks v4.0” (training course). June 13-15, 2016. Ljubljana, **Slovenia**.
- ◆ “Advanced IPv6 Network Reconnaissance”. **IPv6 Business Conference**. June 16, 2016. Zürich, **Switzerland**.
- ◆ “Security and Privacy Implications of Numeric Identifiers Employed in Network Protocols”. **IETF 95**. April 3-8, 2016. Buenos Aires, **Argentina**.
- ◆ “Requirements for IPv6 Enterprise Firewalls”. **IETF 95**. April 3-8, 2016. Buenos Aires, **Argentina**.
- ◆ “Network Ingress Filtering: Defeating Attacks which employ Forged ICMP/ICMPv6 Error Messages”. **IETF 95**. April 3-8, 2016. Buenos Aires, **Argentina**.
- ◆ “On Firewalls in Network Security”. **IETF 95**. April 3-8, 2016. Buenos Aires, **Argentina**.
- ◆ “Operational Implications of IPv6 Packets with Extension Headers”. **IETF 95**. April 3-8, 2016. Buenos Aires, **Argentina**.

- ◆ “Estructura de la IETF y el Proceso de Estándares de Internet”. **IETF 95**. April 3-8, 2016. Buenos Aires, **Argentina**.
- ◆ “Advanced IPv6 Network Reconnaissance”. **IPv6 Security Summit @ Troopers16**. March 14-15, 2016. Heidelberg, **Germany**.
- ◆ “Recent IPv6 Standardization Efforts”. **IPv6 Security Summit @ Troopers16**. March 14-15, 2016. Heidelberg, **Germany**.
- ◆ “Reconocimiento de Redes IPv6”. **Security Day 2015**. December 18, 2015. Guayaquil, **Ecuador**.
- ◆ “Desafíos en Seguridad IPv6”. **Security Day 2015**. December 18, 2015. Guayaquil, **Ecuador**.
- ◆ “Security and Privacy in Internet Protocols” (invited presentation). **NAIST**. November 12, 2015. Nara, **Japan**.
- ◆ “Security Implications of IPv6 Addressing”. **LACNOG 2015**. Sep 28-Oct 2, 2015. Bogota, **Colombia**.
- ◆ “On Firewalls in Network Security”. **IETF 94**. November 1-6, 2015. Yokohama, **Japan**.
- ◆ “Operational Implications of IPv6 Packets with Extension Headers”. **IETF 94**. November 1-6, 2015. Yokohama, **Japan**.
- ◆ “Observations on the Dropping of Packets with IPv6 Extension Headers in the Real World”. **IETF 94**. November 1-6, 2015. **Yokohama, Japan**.
- ◆ “IPv6 Universal Extension Header”. **IETF 94**. November 1-6, 2015. Yokohama, **Japan**.
- ◆ “Transmission and Processing of IPv6 Options”. **IETF 94**. November 1-6, 2015. Yokohama, **Japan**.
- ◆ “Transmission and Processing of IPv6 Options”. **IETF 93**. July 19-24, 2015. Prague, **Czech Republic**.
- ◆ “Desafíos en Seguridad IPv6”. **CIBER 2015**. October 6-7, 2015. Buenos Aires, **Argentina**.
- ◆ “Seguridad IPv6”. **LACNOG 2015**. Sep 28-Oct 2, 2015. Bogota, **Colombia**.
- ◆ “State of the Art in IPv6 Attack & Defense” (training course). **IPv6 Business Conference**. June 18, 2015. Zürich, **Switzerland**.
- ◆ “Hacking IPv6 Networks v3.0” (training course). June 15-17, 2015. Ljubljana, **Slovenia**.
- ◆ “IPv6 Extension Headers in the Wild”. **10th SLO IPv6 Summit**. June 9th, 2015. Ljubljana, **Slovenia**.
- ◆ “Reflections on IPv6 Security”. **10th SLO IPv6 Summit**. June 9th, 2015. Ljubljana, **Slovenia**.
- ◆ “Advanced IPv6 Hacking” (training course). June 8, 11, & 12, 2015. Ljubljana, **Slovenia**.
- ◆ “Security Assessment and Troubleshooting with SI6 IPv6 Toolkit v2.0 (Guille)”. **FLIP6 2015**. Mayo 18-22, 2015. Lima, **Peru**.
- ◆ “Recent Advances in IPv6 Security”. **FLIP6 2015**. Mayo 18-22, 2015. Lima, **Peru**.
- ◆ “Introducción y Experiencias en el IETF”. **III Encuentro Nacional de Técnicos (CABASE)**. April 20-21, 2015. Buenos Aires, **Argentina**.
- ◆ “Recommendations on filtering of IPv6 packets containing IPv6 Extension Headers”. **IETF 92**. March 22-27, 2015. Dallas, Texas, **U.S.A.**
- ◆ “Observations on IPv6 EH Filtering in the Real World”. **IETF 92**. March 22-27, 2015. Dallas, Texas, **U.S.A.**
- ◆ “Transmission and Processing of IPv6 Options”. **IETF 92**. March 22-27, 2015. Dallas, Texas, **U.S.A.**
- ◆ “Current Issues with DNS Configuration Options for SLAAC”. **IETF 92**. March 22-27, 2015. Dallas, Texas, **U.S.A.**
- ◆ “Network Ingress Filtering: Defeating Attacks which employ Forged ICMP/ICMPv6 Error Messages”. **IETF 92**. March 22-27, 2015. Dallas, Texas, **U.S.A.**
- ◆ “New Features in the SI6 Networks' IPv6 Toolkit”. **IPv6 Security Summit 2015**. March 16-17, 2015. Heidelberg, **Germany**.

- ◆ “Recent IPv6 Security Standardization Efforts”. **IPv6 Security Summit 2015**. March 16-17, 2015. Heidelberg, **Germany**.
- ◆ “State of the Art in IPv6 Attack & Defense”. **IT-DEFENSE 2015**. February 4-6, 2015. Leipzig, **Germany**.
- ◆ “Hacking IPv6 Networks v3.0” (training course). **IT-DEFENSE 2015**. February 4-6, 2015. Leipzig, **Germany**.
- ◆ “IPv6 Extension Headers in the Real World”. **IETF 91**. November 9-14, 2014. Honolulu, Hawaii, **U.S.A.**
- ◆ “Transmission and Processing of IPv6 Options”. **IETF 91**. November 9-14, 2014. Honolulu, Hawaii, **U.S.A.**
- ◆ “Deprecating the Generation of IPv6 Atomic Fragments”. **IETF 91**. November 9-14, 2014. Honolulu, Hawaii, **U.S.A.**
- ◆ “Recommendation on Stable IPv6 Interface Identifiers” (6lo wg). **IETF 91**. November 9-14, 2014. Honolulu, Hawaii, **U.S.A.**
- ◆ “Recommendation on Stable IPv6 Interface Identifiers” (6man wg). **IETF 91**. November 9-14, 2014. Honolulu, Hawaii, **U.S.A.**
- ◆ “IPv6 Extension Headers in the Real World v3.0”. **IEPG 91**. November 9, 2014. Honolulu, Hawaii, **U.S.A.**
- ◆ “IPv6-related work at the IETF”. LACNOG meeting, **LACNIC 22**. October 27-31, 2014. Santiago, **Chile**.
- ◆ “State of the Art in IPv6 Security”. **H2HC 2014**. October 18-19, 2014. Sao Paulo, **Brazil**.
- ◆ “Network Security Defense”. **8th Regional CaribNOG Meeting**. September 29-October 3, 2014. Willemstad, **Curacao**.
- ◆ “Security Implications of IPv6 Addressing”. **IEAR 2014**. September 5, 2014. Buenos Aires, **Argentina**.
- ◆ “Recommendations on filtering of IPv6 packets containing IPv6 Extension Headers”. **IETF 90**. July 20-25, 2014. Toronto, **Canada**.
- ◆ “Requirements for IPv6 Enterprise Firewalls”. **IETF 90**. July 20-25, 2014. Toronto, **Canada**.
- ◆ “IPv6 Extension Headers in the Real World v2.0”. **IEPG 90**. July 20, 2014. Toronto, **Canada**.
- ◆ “IPv6 Toolkit v2.0”. **IEPG 90**. July 20, 2014. Toronto, **Canada**.
- ◆ “IPv6 Security & Hacking” (training course). June 9-11, 2014. Ljubljana, **Slovenia**.
- ◆ “Most Recent Advances in IPv6 Security”. **IPv6 Summit 2014**. June 12, 2014. Ljubljana, **Slovenia**.
- ◆ “IPv6 Network Security Assessment and Trouble-shooting”. **IPv6 Summit 2014**. June 12, 2014. Ljubljana, **Slovenia**.
- ◆ “IPv6 Fragmentation and IPv6 Extension Headers in the Real World”. **IPv6 Kongress 2014**. May 22-23, 2014. Frankfurt, **Germany**.
- ◆ “IPv6 Fragmentation and IPv6 Extension Headers in the Real World”. **FLIP6**, LACNIC 21. May 4-9, 2014. Cancun, **Mexico**.
- ◆ “Practical Security Assessment of IPv6 Networks and Devices”. **IPv6 Security Summit**, Troopers 14. March 17-18, 2014. Heidelberg, **Germany**.
- ◆ “Recent IPv6 Security Standardization Efforts”. **IPv6 Security Summit**, Troopers 14. March 17-18, 2014. Heidelberg, **Germany**.
- ◆ “Recommendation on Stable IPv6 Interface Identifiers”. **IETF 89**. March 2-7, 2014. London, **U.K.**
- ◆ “IPv6 Universal Extension Header”. **IETF 89**. March 2-7, 2014. London, **U.K.**
- ◆ “A Small Update on the Use of IPv6 Extension Headers”. **IEPG 89**. March 2, 2014. London, **U.K.**
- ◆ “Advances in IPv6 Security” (Remote presentation). **SP Security Forum**. February 7, 2014. Brussels, **Belgium**.
- ◆ “Security Implications of IPv6 Addressing” (Remote presentation). **SP Security Forum**. February 7, 2014. Brussels, **Belgium**.

- ◆ “Five Security Myths a CISO Should Be Aware of”. **CISO Platform Annual Summit**. November 15-16, 2013. Mumbai, **India**.
- ◆ “Why Should You Worry About IPv6 Security Even If Your Network Runs On IPv4?”. **CISO Platform Annual Summit**. November 15-16, 2013. Mumbai, **India**.
- ◆ “Deprecating EUI-64 Based IPv6 Addresses”. **IETF 88**. November 3-8, 2013. Vancouver, BC, **Canada**.
- ◆ “Security Assessment of Neighbor Discovery (ND) for IPv6”. **IETF 88**. November 3-8, 2013. Vancouver, BC, **Canada**.
- ◆ “On the Validation of TCP Sequence Numbers”. **IETF 88**. November 3-8, 2013. Vancouver, BC, **Canada**.
- ◆ “Fragmentation and Extension Header Support in the IPv6 Internet”. **IEPG 88**. November 3, 2013. Vancouver, BC, **Canada**.
- ◆ “Past, present, and future of IPv6 fragmentation and Extension Headers”. **LACNIC 20**. October 28-November 1, 2013. Willemstad, **Curacao**.
- ◆ “A method for Generating Stable Privacy-Enhanced Addresses with IPv6 SLAAC”. **IETF 87**. July 28-August 2, 2013. Berlin, **Germany**.
- ◆ “Security Assessment of Neighbor Discovery (ND) for IPv6”. **IETF 87**. July 28-August 2, 2013. Berlin, **Germany**.
- ◆ “On the Validation of TCP Sequence Numbers”. **IETF 87**. July 28-August 2, 2013. Berlin, **Germany**.
- ◆ “IPv6 Toolkit News”. **IPv6 Hackers #1**. July 30, 2013. Berlin, **Germany**.
- ◆ “IPv6 Addresses on the DNS”. **IPv6 Hackers #1**. July 30, 2013. Berlin, **Germany**.
- ◆ “Hacking IPv6 Networks version 2.0” (training). **Hack In Paris 2013**, June 17-21, 2013. Paris, **France**.
- ◆ “Security Assessment of IPv6 Networks and Firewalls” (presented with Marc Heuse). **IPv6 Kongress**, June 6-7, 2013, Frankfurt, **Germany**.
- ◆ “IPv6 Network Reconnaissance: Theory and Practice”. **CONFidence 2013**, May 28-29, 2013. Krakow, **Poland**.
- ◆ “IPv6 Hacking Crash Course” (training). **CONFidence 2013**, May 27, 2013. Krakow, **Poland**.
- ◆ “Avances recientes en seguridad IPv6”. **FLIP6 2013**. May 5-10, 2013. Medellín, **Colombia**.
- ◆ “IPv6 Network Reconnaissance: Theory & Practice”. **LACSEC 2013**. May 5-10, 2013. Medellín, **Colombia**.
- ◆ “IPv6 Toolkit: Security Assessment and Trouble-shooting of IPv6 Networks”. **FLIP6 2013**. May 5-10, 2013. Medellín, **Colombia**.
- ◆ “Aspectos de seguridad a considerar con IPv6”. **CUDI - Reunión de Primavera 2013**. April 15-17, 2013. Querétaro, **Mexico**.
- ◆ “Resultados de un Análisis de Seguridad de IPv6”. **XI Foro de Seguridad de RedIRIS**. April 25-26, 2013. Madrid, **Spain**.
- ◆ “Security Assessment of Neighbor Discovery (ND) for IPv6”. **IETF 86**. March 10-15, 2013. Orlando, Florida, **U.S.A.**
- ◆ “Security Implications of IPv6 Options of Type 10xxxxxx”. **IETF 86**. March 10-15, 2013. Orlando, Florida, **U.S.A.**
- ◆ “A method for Generating Stable Privacy-Enhanced Addresses with IPv6 SLAAC”. **IETF 86**. March 10-15, 2013. Orlando, Florida, **U.S.A.**
- ◆ “On the Validation of TCP Sequence Numbers”. **IETF 86**. March 10, 2013. Orlando, Florida, **U.S.A.**
- ◆ “IPv6 Network Reconnaissance: Theory & Practice”. **IEPG 86**. March 10, 2013. Orlando, Florida, **U.S.A.**
- ◆ “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 – Edición 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 Seguridad 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”, **73<sup>rd</sup> IETF Meeting**, November 16-21, 2008. Minneapolis, MN, **USA**.
- ◆ “ICMP attacks against TCP”, **73<sup>rd</sup> IETF Meeting**, November 16-21, 2008. Minneapolis, MN, **USA**.
- ◆ “On the generation of TCP timestamps”, **73<sup>rd</sup> IETF Meeting**, November 16-21, 2008. Minneapolis, MN, **USA**.
- ◆ “On the implementation of TCP urgent data”, **73<sup>rd</sup> IETF Meeting**, November 16-21, 2008. Minneapolis, MN, **USA**.
- ◆ “Security Assessment of the Internet Protocol version 4”, **73<sup>rd</sup> IETF Meeting**, November 16-21, 2008. Minneapolis, MN, **USA**.
- ◆ “Recommendations for filtering ICMP messages”, **73<sup>rd</sup> IETF Meeting**, November 16-21, 2008. Minneapolis, MN, **USA**.
- ◆ “Security implications of Network Address Translators (NATs)”, **73<sup>rd</sup> 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)”, **67<sup>th</sup> IETF Meeting**, November 5-10, 2006, San Diego, CA, **U.S.A.**
- ◆ “ICMP attacks against TCP”, **67<sup>th</sup> IETF Meeting**, November 5-10, 2006, San Diego, CA, **U.S.A.**
- ◆ “NAT Behavioral Requirements for ICMP”, **67<sup>th</sup> 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”, **64<sup>th</sup> IETF Meeting**, November 6-11, 2005, Vancouver, BC, **Canada**.
- ◆ “TCP’s reaction to soft errors”, **64<sup>th</sup> IETF Meeting**, November 6-11, 2005, Vancouver, BC, **Canada**.
- ◆ “TCP User Timeout Option”, **64<sup>th</sup> IETF Meeting**, November 6-11, 2005, Vancouver, BC, **Canada**.

## Webinars

- ◆ “IPv6 Network Reconnaissance”. July 14, 2021. Available at: [https://www.youtube.com/watch?v=R9ztxVO\\_vUc](https://www.youtube.com/watch?v=R9ztxVO_vUc)
- ◆ “Reconocimiento de Redes IPv6”. July 7, 2021. Available at: <https://www.youtube.com/watch?v=zBoudX4Ofdk>
- ◆ “IPv6 Security”. June 30, 2021. Available at: [https://www.youtube.com/watch?v=SiAf\\_AbZGP8](https://www.youtube.com/watch?v=SiAf_AbZGP8)
- ◆ “Seguridad IPv6”. June 23, 2021. Available at: <https://www.youtube.com/watch?v=wQE-yhfD9ac>
- ◆ “IPv6 Mythology”. June 9, 2021. Available at: <https://www.youtube.com/watch?v=2dJa4tdufbA>
- ◆ “IPv6: Mitor y Realidades”. June 1, 2021. Available at: <https://www.youtube.com/watch?v=hlMn0Jlf61Y>

## Participation in Program Committees

- ◆ **LACSEC 2017 - 12o Evento de Seguridad en Redes para América Latina y el Caribe** (in the context of LACNIC 27). May 2017, Foz de Iguazu, Brazil. **Chair** of the Program Committee.
- ◆ **LACSEC 2016 - 11o Evento de Seguridad en Redes para América Latina y el Caribe** (in the context of LACNIC 25). May 2016, Havana City, Cuba. **Chair** of the Program Committee.
- ◆ **IPv6 Hackers #2 meeting**. July 21, 2015. Berlin, Germany. **Organizer**.

- ◆ **LACSEC 2015** - 10o Evento de Seguridad en Redes para América Latina y el Caribe (in the context of **LACNIC 23**). May 2015, Lima, Peru. **Chair** of the Program Committee.
- ◆ **IPv6 Hackers #1 meeting**. July 30, 2013. Berlin, Germany. **Organizer**.
- ◆ **LACSEC 2014** - 9no Evento de Seguridad en Redes para América Latina y el Caribe (in the context of **LACNIC 19**). May 2014, Cancun, Mexico. **Chair** of the Program Committee.
- ◆ **LACSEC 2013** - 8vo Evento de Seguridad en Redes para América Latina y el Caribe (in the context of **LACNIC 19**). May 2013, Medellín, Colombia. **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**). May 2012, Quito, Ecuador. **Chair** of the Program Committee.
- ◆ **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 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.
- ◆ **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.
- ◆ **IEEE 18th International Conference on Computer Communications and Networks (ICCCN 2009)**, Track on Network Architecture and Protocols (NAP). Available at: <http://iccn.org/iccn09/tracks/nap.html>

## 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.

- ◆ Deering, S., Hinden, R., “**Internet Protocol, Version 6 (IPv6) Specification**”, **IETF RFC8200**. July 2017. Available at: <https://tools.ietf.org/rfc/rfc8200.txt>
- ◆ Baker, F., “Testing Eyeball Happiness”, **IETF RFC 6556**. April 2012. Available at: <https://www.rfc-editor.org/rfc/rfc6556.txt>
- ◆ 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>
- ◆ Kaeo, 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.

- ◆ 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:**

- ◆ Performed a technical review of three chapters about TCP/IP network programming of the book “**The Linux Programing 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.
- ◆ 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](http://www.tcpipguide.com/free/t_Acknowledgments.htm))
- ◆ Performed a technical review of the book “**Patterns in Network Architecture**”, authored by **John Day**. I received the corresponding credit in the preface of the book.
- ◆ 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.

- ◆ Wrote exercises 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”.
- ◆ 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 ([http://ftp.prenhall.com/pub/esm/sample\\_chapters/cs/stallings/pdf/preface.pdf](http://ftp.prenhall.com/pub/esm/sample_chapters/cs/stallings/pdf/preface.pdf)).
- ◆ Wrote exercises and performed a technical review of all the chapters of the book “**Operating Systems**”, authored by **William Stallings**. I received the corresponding credit in the “Acknowledgements” section of the book.
- ◆ 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.
- ◆ 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:

- ◆ **F5's K09940637: NTP vulnerability CVE-2019-11331** (<https://support.f5.com/csp/article/K09940637>)
- ◆ **RedHat Security Advisory RHSA-2011:1465-1: Important: kernel security and bug fix update** (<https://rhn.redhat.com/errata/RHSA-2011-1465.html>)
- ◆ **Ubuntu: USN-1253-1: Linux kernel vulnerabilities** (<https://ubuntu.com/security/notices/USN-1253-1>)
- ◆ **SUSE Security Announcement: Linux kernel security update** (SUSE-SA:2011:046) (<https://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)** (<https://www.sifnetworks.com/files/advisories/al-20050412-00308.pdf> and <https://www.sifnetworks.com/files/advisories/re-20050412-00303.pdf>)
- ◆ **US-CERT: TCP/IP implementations do not adequately validate ICMP error messages** (<https://www.kb.cert.org/vuls/id/222750>)
- ◆ **Cisco Systems: Crafted ICMP Messages Can Cause Denial of Service** ( )
- ◆ **Microsoft Corp.: Microsoft Security Bulletin Summary for April 2005** (<http://www.microsoft.com/technet/security/bulletin/ms05-apr.msp>)
- ◆ **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>)

## Open Source Tools

As part of my work in the area of communications protocols security, I have released the following open-source security assessment tools:

- ◆ **SI6 Networks' IPv6 Toolkit:** The only portable (and publicly-available) IPv6 security assessment toolkit. Available at: <https://www.si6networks.com/tools/ipv6toolkit> . This toolkit has been incorporated into the Debian GNU/Linux package system (ipv6toolkit) and in the Kali Linux distribution.
- ◆ **SI6 Networks' IoT Toolkit:** A security assessment toolkit for the Internet of Things (IoT). Available at: <https://www.si6networks.com/tools/iot-toolkit>
- ◆ **ipv6mon:** An IPv6 address monitoring daemon. Available at: <https://www.si6networks.com/tools/ipv6mon>
- ◆ **ICMP tools:** A set of ICMPv4 security assessment tools. Available at: <https://www.si6networks.com/tools>

## Open Source Contributions

As part of my work in the area of communications protocols security, I have contributed code to a variety of open source projects:

- ◆ **Linux kernel:** Implementation of IETF RFC 8981.
- ◆ **FreeBSD kernel:** Implementation of IETF RFC 8981.
- ◆ **NetworkManager:** Implementation of IETF Internet-Draft draft-gont-6man-slaac-renum,
- ◆ **systemd-networkd:** Implementation of IETF Internet-Draft draft-gont-6man-slaac-renum.
- ◆ **OpenBSD slaacd(8):** Implementation of IETF Internet-Draft draft-gont-slaac-renum. Reduction of Valid Lifetimes of IPv6 temporary addresses.
- ◆ **OpenBSD kernel:** Implementation of the mitigation for ICMP-based performance -degrading attacks in RFC5927.
- ◆ **OpenBSD rad(8):** Implementation of IETF Internet-Draft draft-gont-6man-slaac-renum.

## Press

My work in the area of communications protocols security has been featured in the following articles and interviews:

- ◆ **Revista Brando:** *Los ingenieros de la matrix: ¿quién ordena internet?* (<https://www.lanacion.com.ar/lifestyle/los-ingenieros-de-la-matrix-quien-ordena-internet-nid1921463/>)
- ◆ **LightReading:** *Industry Mobilizes on Latest TCP Flaw* (<https://www.lightreading.com/ethernet-ip/industry-mobilizes-on-latest-tcp-flaw/d/d-id/612378>)
- ◆ **The Register:** *IPv6 vulnerable to fragmentation attacks that threaten core internet routers.* ([https://www.theregister.com/2017/01/18/net\\_boffin\\_ipv6\\_needs\\_hardening\\_against\\_fragmentation\\_attacks/](https://www.theregister.com/2017/01/18/net_boffin_ipv6_needs_hardening_against_fragmentation_attacks/))
- ◆ **Golem.de:** *Interview Fernando Gont zur Sicherheit in IPv6* ([https://www.youtube.com/watch?v=i\\_IUXBagvIc](https://www.youtube.com/watch?v=i_IUXBagvIc))
- ◆ **TechTarget.com:** *Lagging Security Features, Vulnerabilities Could Hamper Transition to New Internet* (<https://bit.ly/3qHXFgW>)
- ◆ **TechTarget.com:** *World IPv6 recap* (<https://bit.ly/3fE1FK5>)
- ◆ **Network World:** *Future-Net Debrief* (<https://www.networkworld.com/article/2230740/cisco-subnet-future-net-debrief.html>)

- ◆ **Prensa LACNIC:** *Fernando Gont - IPv6 - LACNOG 2011* (<https://www.youtube.com/watch?v=Ta1iwffclIA>)
- ◆ **SecurityFocus:** *U.K. response team releases Net security guide* (<https://bit.ly/3nF8vIF>)
- ◆ **The Register:** *IP security shortcomings unpicked* ([https://www.theregister.com/2009/02/17/ip\\_security\\_review/](https://www.theregister.com/2009/02/17/ip_security_review/))
- ◆ **IT News:** *UK government blast TCP/IP security* (<https://www.itnews.com.au/news/uk-government-blast-tcp-ip-security-120418>)
- ◆ **UK's National Infrastructure Security Co-ordination Centre:** *NISCC - the Quarterly (01/06)* (<https://www.si6networks.com/files/press/re-20060818-00564.pdf>)
- ◆ **CNET News:** *Bug hunters, software firms in uneasy alliance* (<https://www.cnet.com/news/privacy/bug-hunters-software-firms-in-uneasy-alliance/>)
- ◆ **SecurityFocus:** *Big debate over small packets* (<https://bit.ly/3rxpQhv>)
- ◆ **KernelTrap:** *OpenBSD Hackathon 2005, Part III* (<https://bit.ly/3NjGoCZ>)
- ◆ **SecurityFocus:** *OpenBSD's network stack* (<https://bit.ly/3FSU0mc>)

## Recent positions held

### 2022:

Security researcher and consultant at **SI6 Networks** (<https://www.si6networks.com>). My activities include: security assessment of communication protocols, vulnerability research, production of security assessment tools, design and implementation of counter-measures, communications protocols standardization, Internet engineering, and information security consulting.