BSDCan 2012 Presentation Proposal

Presentation title:

Recent advances in IPv6 Security

Speaker:

Fernando Gont

Extended abstract:

The IPv6 protocol suite was designed to accommodate the present and future growth of the Internet, and is expected to be the successor of the original IPv4 protocol suite. It has already been deployed in a number of production environments, and many organizations have already scheduled or planned its deployment in the next few years. Additionally, a number of activities such as the World IPv6 Day in 2011 and the upcoming World IPv6 Launch Day (scheduled for June 2012) have led to an improvement in IPv6 awareness and an increase in the number of IPv6 deployments.

There are a number of factors that make the IPv6 protocol suite interesting from a security standpoint. Firstly, being a new technology, technical personnel has much less confidence with the IPv6 protocols than with their IPv4 counterpart, and thus it is more likely that the security implications of the protocols be overlooked when the protocols are deployed. Secondly, IPv6 implementations are much less mature than their IPv4 counterparts, and thus it is very likely that a number of vulnerabilities will be discovered in them before their robustness matches that of the existing IPv4 implementations. Thirdly, security products such as firewalls and NIDS's (Network Intrusion Detection Systems) usually have less support for the IPv6 protocols than for their IPv4 counterparts, either in terms of features or in terms of performance. Fourthly, the security implications of IPv6 transition/co-existence technologies on existing IPv4 networks are usually overlooked, potentially enabling attackers to leverage these technologies to circumvent IPv4 security measures in unexpected ways.

During the last few years, the UK CPNI (Centre for the Protection of National Infrastructure) carried out the first comprehensive security assessment of the Internet Protocol version 6 (IPv6) and related technologies (such as transition/co-existence mechanisms). The result of the aforementioned project is a series of documents that provide advice both to programmers implementing the IPv6 protocol suite and to network engineers and security administrators deploying or operating the protocols. Part of the results of the aforementioned project have been recently published, leading to a number of improvements in many IPv6 implementations.

Fernando Gont will discuss the results of the aforementioned project, introducing the attendees to the "state of the art" in IPv6 security, and providing advice on how to deploy the IPv6 protocols securely. Gont will also discusss recent advances in IPv6 security areas such as Denial of Service attacks, firewall circumvention, and Network Reconnaissance, and will describe other IPv6 security areas in which further work is needed. Additionally, he will demonstrate the use of some attack/assessment tools that implement new network reconnaissance techniques or that exploit a number of vulnerabilities found in popular IPv6 implementations.

References:

The following publications support the aforementioned presentation:

- 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., “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., “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., “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., “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

Fernando Gont's contact information & bio

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

web:
Personal: http://www.gont.com.ar
Company: http://www.si6networks.com

Cell-phone:
+54 9 11 6536 4380

Telephone:
+54 11 4650 8472

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

Country of origin:
Argentina

Employer and/or affiliations:
SI6 Networks (http://www.si6networks.com)
Universidad Tecnológica Nacional/Facultad Regional Haedo (Argentina).
Research project carried out on behalf of the United Kingdom's Centre for the Protection of National Infrastructure (UK CPNI).

Brief biography:

Fernando Gont specializes in the field of communications protocols security, working for private and governmental organizations.

Gont has worked on a number of projects for the UK National Infrastructure Security Co-ordination Centre (NISCC) and the UK Centre for the Protection of National Infrastructure (CPNI) in the field of communications protocols security. As part of his work for these organizations, he has written a series of documents with recommendations for network engineers and implementers of the TCP/IP protocol suite, and has performed the first thorough security assessment of the IPv6 protocol suite.

Gont is currently working as a security consultant and researcher for SI6 Networks (http://www.si6networks.com). Additionally, he is a member of the Centro de Estudios de Informatica (CEDI) at Universidad Tecnológica Nacional/Facultad Regional Haedo (UTN/FRH) of Argentina, where he works in the field of Internet engineering. As part of his work, he is active in several working groups of the Internet Engineering Task Force (IETF), and has published a number of IETF RFCs (Request For Comments) and Internet-Drafts. Gont is also a member of the Transport Directorate of the IETF (http://trac.tools.ietf.org/area/tsv/trac/wiki/TSV-Directorate).

Gont has been a speaker at a number of conferences and technical meetings about information security, operating systems, and Internet engineering, including: CanSecWest

2005, Midnight Sun Vulnerability and Security Workshop/Retreat 2005, FIRST Technical Colloquium 2005, Kernel Conference Australia 2009, DEEPSEC 2009, HACK.LU 09, IETF 73, IETF 76, LACNIC XII, Hack In Paris 2011, HACK.LU 2011, and DEEPSEC 2011.

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

List of publications:

Please find this information in the attached Curriculum Vitae (CV).

Talks:

Please find this information in the attached Curriculum Vitae (CV).