novática
Revista de la Asociación de Técnicos de Informática

Novática, revista fundada en 1975 y decana de la prensa informática española, es el órgano oficial de expresión y formación continua de **ATI** (Asociación de Técnicos de Informática), organización que edita también la revista **REICIS** (Revista Española de Innovación, Calidad e Ingeniería del Software).

<http://www.ati.es/novatica/>
<http://www.ati.es/reicis/>

ATI es miembro fundador de **CEPIS** (*Council of European Professional Informatics Societies*) y es representante de España en **IFIP** (*International Federation for Information Processing*); tiene un acuerdo de colaboración con **ACM** (*Association for Computing Machinery*), así como acuerdos de vinculación o colaboración con **AdaSpain**, **AI2**, **ASTIC**, **RITSI** e **Hispalinux**, junto a la que participa en **ProInnova**.

Consejo Editorial
Ignacio Agulló Sousa, Guillem Alsina González, María José Escalona Cuaresma, Rafael Fernández Calvo (presidente del Consejo), Jaime Fernández Martínez, Luís Fernández Sanz, Dídac Lopez Viñas, Celestino Martín Alonso, José Onofre Montesa Andrés, Francesc Noguera Puig, Ignacio Pérez Martínez, Andrés Pérez Payeras, Víktu Pons i Colomer, Juan Carlos Vigo López

Coordinación Editorial
Llorenç Pagés Casas <pages@ati.es>
Composición y autoedición
Jorge Llácer Gil de Ramales
Traducciones
Grupo de Lengua e Informática de ATI <http://www.ati.es/gt/lengua-informatica/>
Administración
Tomás Brunete, María José Fernández, Enric Camarero

Secciones Técnicas - Coordinadores
Acceso y recuperación de la Información
José María Gómez Hidalgo (Optenet), <jmgomezh@yahoo.es>
Manuel J. Maña López (Universidad de Huelva), <manuel.mana@diesia.uhu.es>
Administración Pública electrónica
Francisco López Crespo (MAE), <flc@ati.es>
Sebastià Justicia Pérez (Diputación de Barcelona) <sjusticia@ati.es>
Arquitecturas
Enrique F. Torres Moreno (Universidad de Zaragoza), <enrique.torres@unizar.es>
José Flich Cardo (Universidad Politécnica de Valencia, <jflich@disca.upv.es>
Auditoría SITIC
Marina Touriño Troitiño, <marinatourino@marinatourino.com>
Sergio Gómez-Landero Pérez (Endesa), <sergio.gomezlandero@endesa.es>
Derecho y tecnologías
Isabel Hernando Collazos (Fac. Derecho de Donostia, UPV), <isabel.hernando@ehu.es>
Elena Davara Fernández de Marcos (Davara & Davara), <edavara@davara.com>
Enseñanza Universitaria de la Informática
Cristóbal Pareja Flores (DSIP-UCM), <cpareja@sip.ucm.es>
J. Ángel Velázquez Iturbide (DLSI I, URJC), ángel.velazquez@urjc.es>
Entorno digital personal
Andrés Marín López (Univ. Carlos III), <amarin@it.uc3m.es>
Diego Gachet Páez (Universidad Europea de Madrid), <gachet@uem.es>
Estándares Web
Encarna Quesada Ruiz (Virati), <encarna.quesada@virati.com>
José Carlos del Arco Prieto (TCP Sistemas e Ingeniería), <jcarco@gmail.com>
Gestión del Conocimiento
Joan Baiget Solé (Cap Gemini Ernst & Young), <joan.baiget@ati.es>
Gobierno Coorporativo de las TI
Manuel Palao García-Suelto (ATI), <manuel@palao.com>,
Miguel García-Menéndez (ITTI) <mgarciamenendez@ittrendsinstitute.org>
Informática y Filosofía
José Angel Olivas Varela (Escuela Superior de Informática, UCLM), <joseangel.olivas@uclm.es>
Roberto Feltrero Oreja (UNED), <rfeltrero@gmail.com>
Informática Gráfica
Miguel Chover Sellés (Universitat Jaume I de Castellón), <chover@lsi.uji.es>
Roberto Vivó Hernando (Eurographics, sección española), <rvivo@dsic.upv.es>
Ingeniería del Software
Javier Dolado Cosín (DLSI-UPV), <dolado@si.ehu.es>
Daniel Rodríguez García (Universidad de Alcalá), <daniel.rodriguez@uah.es>
Inteligencia Artificial
Vicente Botti Navarro, Vicente Julián Inglada (DSIC-UPV), <{vbotti,vinglada}@dsic.upv.es>
Interacción Persona-Computador
Pedro M. Latorre Andrés (Universidad de Zaragoza, AIPO), <platorre@unizar.es>
Francisco L. Gutierrez Vela (Universidad de Granada, AIPO), <fgutierr@ugr.es>
Lengua e Informática
M. del Carmen Ugarte García (ATI), <cugarte@ati.es>
Lenguajes informáticos
Óscar Belmonte Fernández (Univ. Jaime I de Castellón), <belfern@lsi.uji.es>
Inmaculada Coma Tatay (Univ. de Valencia), <Inmaculada.Coma@uv.es>
Lingüística computacional
Xavier Gómez Guinovart (Univ. de Vigo), <xgg@uvigo.es>
Manuel Palomar (Univ. de Alicante), <mpalomar@dlsi.ua.es>
Mundo estudiantil y jóvenes profesionales
Federico G. Mon Trotti (RITSI), <gnu.fede@gmail.com>
Mikel Salazar Peña (Area de Jovenes Profesionales, Junta de ATI Madrid), <mikeltxo_uni@yahoo.es>
Profesión informática
Rafael Fernández Calvo (ATI), <rfcalvo@ati.es>
Miquel Sárries Griñó (ATI), <miquel@sarries.net>
Redes y servicios telemáticos
José Luis Marzo Lázaro (Univ. de Girona), <joseluis.marzo@udg.es>
Juan Carlos López López (UCLM), <juancarlos.lopez@uclm.es>
Robótica
José Cortés Arenas (Sopra Group), <joscorare@gmail.com>
Juan González Gómez (Universidad cARLOS III), <juan@iearobotics.com
Seguridad
Javier Areitio Bertolín (Univ. de Deusto), <jareitio@deusto.es>
Javier López Muñoz (ETSI Informática-UMA), <jlm@lcc.uma.es>
Sistemas de Tiempo Real
Alejandro Alonso Muñoz, Juan Antonio de la Puente Alfaro (DIT-UPM),
<{aalonso,jpuente}@dit.upm.es>
Software Libre
Jesús M. González Barahona (GSYC - URJC), <jgb@gsyc.es>
Israel Herráiz Tabernero (Universidad Politécnica de Madrid), <isra@herraiz.org>
Tecnología de Objetos
Jesus García Molina (DIS-UM), <jmolina@um.es>
Gustavo Rossi (LIFIA-UNLP Argentina), <gustavo@sol.info.unlp.edu.ar>
Tecnologías para la Educación
Juan Manuel Dodero Beardo (UC3M), <dodero@inf.uc3m.es>
César Pablo Córcoles Briongo (UOC), <ccorcoles@uoc.edu>.
Tecnologías y Empresa
Dídac López Viñas (Universitat de Girona), <didac.lopez@ati.es>
Alonso Álvarez García (TID) <aag@tid.es>
Tendencias tecnológicas
Gabriel Martí Fuentes (Interbits), <gabi@atinet.es>
Juan Carlos Vigo (ATI) <juancarlosvigo@atinet.es>
TIC y Turismo
Andrés Aguayo Maldonado, Antonio Guevara Plaza (Univ. de Málaga), <{aguayo, guevara}@lcc.uma.es>

Las opiniones expresadas por los autores son responsabilidad exclusiva de losmismos. ***Novática*** permite la reproducción, sin ánimo de lucro, de todos los artículos, a menos que lo impida la modalidad de © o copyright elegida por el autor, debiéndose en todo caso citar su procedencia y enviar a ***Novática*** un ejemplar de la publicación.

Coordinación Editorial, Redacción Central y Redacción ATI Madrid
Plaza de España 6, 2ª planta, 28008 Madrid
Tlfn.914029391; fax.913093685 <novatica@ati.es>
Composición, Edición y Redacción ATI Valencia
Av. del Reino de Valencia 23, 46005 Valencia
Tlfn. 963740173 <novatica_prod@ati.es>
Administración y Redacción ATI Cataluña
Via Laietana 46, ppal. 1ª, 08003 Barcelona
Tlfn.934125235; fax 934127713 <secregen@ati.es>
Redacción ATI Andalucía <secreand@ati.es>
Redacción ATI Galicia<secregal@ati.es>
Suscripción y Ventas <novatica.subscripciones@atinet.es>
Publicidad Plaza de España 6, 2ª planta, 28008 Madrid
Tlnf 914029391; fax.913093685 <novatica@ati.es>
Imprenta: Derra S.A., Juan de Austria 66, 08005 Barcelona.
Depósito legal: B 15.154-1975 -- ISSN: 0211-2124; CODEN NOVAEC
Portada: "Mineral, vegetal, animal" - Concha Arias Pérez / © ATI
Diseño: Fernando Agresta / © ATI 2003

Nº 223, mayo-junio 2013, año XXXIX

sumario

Tema del próximo número:
"Eficiencia energética en centros de proceso de datos"

El "caso Snowden" y la seguridad de las redes de telecomunicación

Una de las noticias más relevantes de los últimos meses ha sido el "caso Snowden".

Como es bien sabido, su protagonista ha sido Edward Snowden, un joven profesional informático, ahora exiliado en Rusia, que estuvo empleado en las dos principales agencias de espionaje[1] estadounidenses, la CIA (*Central Intelligence Agency*) y la NSA (*National Security Agency*). En el mes de mayo, Snowden filtró al periódico británico The Guardian detalles de los programas de vigilancia e intrusión masivas sobre las redes de telecomunicaciones de todo el mundo llevados a cabo por la citada NSA en colaboración con sus homólogas británica GCHQ (*Government Communications Headquarters*) y alemana BND (*Bundesnachrichtendienst*); también, según analistas bien informados, con otras agencias de espionaje de países aliados de los EEUU.

Este asunto puede ser contemplado desde muchos puntos de vista, por ejemplo sus aspectos políticos, su impacto sobre la privacidad, el difícil equilibrio entre libertad y seguridad e incluso la opinión que se pueda tener sobre Snowden (¿un traidor a su patria?, ¿un oportunista ansioso de notoriedad?, ¿un defensor de los derechos a la intimida y a la libertad de expresión?). Sin embargo, en este editorial vamos a concentrarnos sobre todo en lo que se refiere a la ruptura por los citados organismos de los sistemas cifrados de seguridad usados para proteger la privacidad de los ciudadanos en el uso de las diversas herramientas de telecomunicación disponibles.

Según The Guardian, los métodos utilizados "*incluyen medidas ocultas para asegurar el control por parte de la NSA de la definición de los estándares internacionales de cifrado, el uso de superordenadores para romper el cifrado por la 'fuerza bruta' y – el secreto mejor guardado de todos – la colaboración con las mismas empresas tecnológicas y proveedores de servicios de Internet. Mediante esta colaboración clandestina, estas agencias habían introducido vulnerabilidades secretas – conocidas como puertas traseras o puertas trampa – en programas comerciales de cifrado*". Y sigue diciendo lo siguiente: "*La NSA hace modificaciones al software y a los dispositivos comerciales de encriptado para poder 'explotarlos' … y obtiene detalles técnicos de sistemas criptográficos comerciales de seguridad de la información a través de sus relaciones con las empresas del sector*".

Estamos hablando de esas mismas empresas que comercializan programas y dispositivos que se ofrecen en el mercado como garantes de la seguridad de ordenadores y redes de de telecomunicaciones. Son empresas que además nos aseguran que nuestros correos electrónicos, nuestras conversaciones telefónicas, nuestros datos bancarios o médicos están cuidadosamente protegidos y no pueden ser descifrados ni por gobiernos ni por delincuentes (en el primer caso a menos que exista una orden judicial que lo permita), puesto que usan protocolos de seguridad de enorme utilización mundial como HTTPS y Secure Sockets Layer (SSL). Sobre ellos, y sobre Voice-Over-IP, han puesto en especial su atención las agencias de espionaje antes citadas y probablemente algunas más con capacidad tecnológica y financiera para hacerlo pero que han tenido la suerte de no ser mencionadas por Snowden.

Se da además la circunstancia de que estos protocolos, programas y dispositivos han sido "hackeados" y ha habido intrusiones masivas en las comunicaciones, principalmente mediante el sistema PRISM, no solamente con el fin, comprensible en alguna medida, de proteger a la gran potencia imperial estadounidense de las amenazas terroristas sino también para fines mucho menos justificables como el espionaje industrial y la interceptación de las comunicaciones de gobernantes y organizaciones de países amigos y aliados, entre ellos la presidenta del Brasil o los comisarios de la Unión Europea.

Existe consenso en la comunidad de Internet sobre que la interoperabilidad global y el carácter abierto de la Red son el fundamento de su utilidad para el avance social y económico del planeta, a la vez que constituyen un elemento esencial para la confianza de los usuarios en la inviolabilidad de sus comunicaciones a través de la misma. Esta confianza está siendo quebrada por la conducta de las citadas agencias de espionaje sin que el principal gobierno implicado, el de los EEUU, haya mostrado su intención de cambiar de conducta.

Por ello es necesario que haya una reacción seria no sólo de los gobiernos y organismos espiados sino, también y sobre todo, de la sociedad civil a través de organizaciones de defensa de los derechos humanos, organizaciones profesionales del mundo de la informática y las telecomunicaciones, de usuarios de Internet, etc.

La gravedad de los hechos denunciados así lo justifica.

La Junta Directiva de ATI

Reacciones sobre este asunto

- Comunicado de la Internet Society: "*Internet Society Responds to Reports of the U.S. Government's Circumvention of Encryption Technology*", <http://www.internetsociety.org/sites/default/files/Internet%20Security%20Statement%20090913.pdf>.
- Comunicado de Privacy International: "*Governments break silence on surveillance as activists launch human rights principles*", <https://www.privacyinternational.org/press-releases/governments-break-silence-on-surveillance-as-activists-launch-human-rights-principles>.

Nota

[1] La palabra "espionaje" ha sido convenientemente sustituida en los últimos años por "inteligencia", más tranquilizante y políticamente correcta.