Revista de Comunicación Vivat Academia
ISSN: 1575-2844 · DOI: http://dx.doi.org/10.15178/va.2001.29.1-14
Octubre 2001 · Año IV · nº 29 · pp. 1-14

¿LIBERTADES A CAMBIO DE SEGURIDAD?

¿LIBERTIES IN EXCHANGE FOR SAFETY?

AUTORES
Jesus Cea Avion: Ingeniero Técnico Superior de Telecomunicaciones. Director Técnico e I+D en HispaSec (España)
jcea@argo.es

CURRÍCULUM VITAE

Ingeniero Técnico Superior de Telecomunicaciones. Director Técnico e I+D en HispaSec, empresa especializada en seguridad informática, consultoría, auditoría y desarrollo. Interesado tanto en los aspectos criptográficos como en las implicaciones sociales y legales del uso de tecnología criptográfica. Miembro de Fronteras Electrónicas España www.arnal.es/free. Más información sobre criptología en la página www.jcea.es/cripto.htm y artículos en www.jcea.es/artic.

RESUMEN

Desde hace años existe un debate en EE.UU. sobre el uso privado de la criptografía para asegurar la confidencialidad de las comunicaciones entre particulares. El argumento de los que están en contra es que si una comunicación está cifrada, las fuerzas del orden no pueden espiarlas para detectar actividades criminales. Proponen o bien prohibir la criptografía por ley, o dotar a los programas criptográficos de Puertas Traseras.

PALABRAS CLAVE

Libertades – Seguridad – Criptografía - Atentados

ABSTRACT

For years there is a debate in the U.S. on the private use of cryptography to ensure confidentiality of communications between individuals. The argument of those against is that if a communication is encrypted, the security forces can not spy on them to identify criminal activity. Proposed ban cryptography or by law, or provide cryptographic programs Backdoors.

KEY WORDS

Freedoms - Security - Cryptography – Attacks

Los atentados recientes en EE.UU. abonan el campo para nuevas leyes que pretenden proporcionar más seguridad a los ciudadanos a costa de un mayor control gubernamental.

A continuación se adjunta un mensaje que escribí hace unas semanas para un foro del que formo parte pero que plantea una evolución previsible en el uso y reconocimiento de libertades civiles, sobre todo en lo que se refiere al binomio

libertad/seguridad. El mensaje se incluye tal y como fue enviado, sin ningún tipo de edición.

Subject: [Nosotros] Debate: ¿libertades a cambio de seguridad?
Date: Tue, 25 Sep 2001 12:32:29 +0200
From: Jesus Cea Avion <jcea@argo.es>

Me gustaría proponer un debate a los contertulios, relativo a los movimientos que se empiezan a oler en EE.UU. tendentes a limitar "algo" las libertades a cambio de una "presunta" mejora en la seguridad.

Elaboraré más mi postura si es necesario a lo largo del debate, si lo hay, pero mi posición personal es que no se puede comerciar con las libertades, y menos para obtener una seguridad adicional más que dudosa. Las libertades que se pierden tardan mucho en recuperarse, o no se recuperan nunca.

Lo peor de todo es que, encima, no veo ninguna razón incontestable para que esa pérdida de libertad incremente la seguridad.

Un ejemplo:

Desde hace años existe un debate en EE.UU. sobre el uso privado de la criptografía para asegurar la confidencialidad de las comunicaciones entre particulares. El argumento de los que están en contra es que si una comunicación está cifrada, las fuerzas del orden no pueden espiarlas para detectar actividades criminales. Proponen o bien prohibir la criptografía por ley, o dotar a los programas criptográficos de "puertas traseras".

ISSN: 1575-2844 · DOI: http://dx.doi.org/10.15178/va.2001.29.1-14

Para cualquier persona "normal y corriente", este argumento tiene su lógica y parece razonable.

Pero no lo es. No lo es por tres razones:

* La gente que usa la criptografía con fines delictivos son delincuentes y, por definición, no seguirán las leyes. Si no existen programas criptográficos, crearán los suyos propios (es muy fácil y existen infinidad de algoritmos de alta calidad documentados en cualquier libro o revista sobre la materia), sin puertas traseras.

* Si el usuario doméstico no puede usar la criptografía, mientras que el delincuente lo hará de todas formas, la seguridad de sus comunicaciones decrecerá. El que nada tiene que ocultar estará a merced del "gran hermano", de organizaciones mafiosas, de terroristas o del trabajador malicioso de su ISP. Esa gente, que no tiene nada que ocultar, estará completamente desprotegida.

Yo no tengo nada que ocultar, pero las cartas que envío a mi madre las mando en un sobre cerrado. ¿Mañana se me obligará a enviar todo en forma de postal, abierto, para que la policía pueda comprobar que no envío los planos de una bomba atómica?. Por cierto, cualquiera que sepa algo de física puede construirse una... si cuenta con los materiales apropiados; no hace falta que nadie le mande los planos.

* Si un programa tiene puertas traseras, ¿Quien controla su uso correcto?. ¿Quien controla que mañana, por ejemplo, un grupo mafioso o terrorista consiga el acceso a dicha puerta?. Sería peor que no tener criptografía, porque piensas que estás seguro cuando no es así.

La criptografía es una tecnología y, como algunos estamos cansados de repetir, la tecnología es neutral. Se puede usar tanto para lo bueno como para lo malo. La

gasolina puede provocar explosiones, incendios y contamina cosa mala, pero no la vamos a prohibir a corto plazo. Los cuchillos provocan numerosos accidentes y son armas utilizadas en la mayoría de los delitos de sangre, y tampoco los vamos a prohibir. ¿Con qué cortaría yo el jamón si no?.

Otro ejemplo evidente es el de la biometría. Se quiere, por ejemplo, desplegar sistemas de reconocimiento facial, escáneres de retina o de huella dactilar a la entrada de un estadio de fútbol, por ejemplo. El objetivo es detectar al momento elementos terroristas y criminales buscados por la policía.

Todo muy bueno y muy bonito.

Por supuesto, en cuanto los criminales sepan que tendrán que pasar por un sistema de ese tipo, sencillamente verán el fútbol desde su casa. El terrorista que quiere poner una bomba se colará por la salida de incendios o sobornará a un guardia... o no estará fichado.

Pero, ¿y el usuario "particular"?

Un día te encontrarás que, cuando llevas a tu hijo al partido, la seguridad del estadio te retiene por tener una multa pendiente o por no haber devuelto tu último libro a la biblioteca. Asimismo, un día te empezará a llegar publicidad sobre botas de fútbol, porque "alguien" ha filtrado que eres un habitual del estadio.

Peor aún, pasado mañana tu compañía aseguradora te subirá las cuotas de tu seguro de vida porque se ha demostrado que asistir a un partido de fútbol incrementa las probabilidades de sufrir un infarto.

ISSN: 1575-2844 · DOI: http://dx.doi.org/10.15178/va.2001.29.1-14

La semana que viene te encontrarás tu coche destrozado porque "alguien" lo ha golpeado con un bate de beisbol. Tu nunca sabrás la razón, pero un hincha del equipo rival del pasado domingo, que perdió en tu campo, vive en tu misma calle y "sabe mucho de internet".

Un tercer punto: se está abogando por incrementar la monitorización de Internet, meter el famoso "carnívoro" para escanear mensajes buscando "cosas inconvenientes", etc. El argumento es que los terroristas usan internet para coordinarse.

Dios, ¡menudo sinsentido!.

Cuando ETA envía un paquete bomba a un periodista, en España, nadie se plantea denunciar a correos y obligarle a analizar todos y cada uno de los paquetes que gestiona. La mayoría de los crímenes se planean por teléfono (no por Internet), y nadie se ha planteado el pinchar absolutamente todas las llamadas sin orden judicial.

¿Por qué Internet es tan diferente?. ¿Por qué ese agravio comparativo?.

En EE.UU., por una vez, ya no son sólo las asociaciones pro derechos civiles las que están preocupadas, sino que muchos ciudadanos (y, afortunadamente, medios de comunicación), se están dando cuenta de que las propuestas de ley que se están debatiendo en la actualidad en EE.UU. son lobos en piel de cordero, y que sus implicaciones a medio y largo plazo son aterradoras.

Las leyes antiterroristas que se plantean, de aprobarse su borrador actual, convertirán EE.UU. en el mayor estado policial que la humanidad haya conocido nunca.

Recomiendo a todos los lectores de "Una Al Día" que lean con atención los documentos que siguen. Considerando el colonialismo cultural de EE.UU. sobre el mundo occidental, habrá que seguir muy de cerca la evolución legislativa en EE.UU., en previsión de una posible exportación a Europa en un futuro más o menos inmediato.

La mayoría de los enlaces han sido recopilados y difundidos por RRE (Red Rock Eater News Service). Nuestro agradecimiento.

Opina sobre esta noticia:

http://www.hispasec.com/unaaldiacom.asp?id=1080

Más información:

Red Rock Eater News Service
http://dlis.gseis.ucla.edu/people/pagre/rre.html
House Bill Would Expand Federal Detention Powers
http://www.washingtonpost.com/wp-dyn/articles/A55410-2001Oct1.html
Defining Terrorism Stirs Words of Dispute
http://www.latimes.com/templates/misc/printstory.jsp?slug=la%2D100101legal
Statement on Terrorism, Civil Liberties, and the Internet
http://www.pfir.org/statements/liberties
Don't Blame the Internet
http://www.washingtonpost.com/wp-dyn/articles/A43828-2001Sep29.html
analysis of the anti-hacking provisions of the proposed anti-terrorism act
http://www.politechbot.com/p-02597.html
British ID Cards Backlash Begins
http://www.guardian.co.uk/humanrights/story/0,7369,561043,00.html

ISSN: 1575-2844 · DOI: http://dx.doi.org/10.15178/va.2001.29.1-14

"Amazing" Lapse in Security Cited at Logan
http://www.boston.com/dailyglobe2/274/metro/_Amazing_lapse_in_security_cited_at_Logan+.shtml
Will Other Voices Be Heard?
http://chicagotribune.com/features/lifestyle/chi-0110010037oct01.story
the very dangerous attacks on Bill Maher
http://www.dailyhowler.com/h100101_1.shtml
Censorship and the War on Terrorism
http://www.mediachannel.org/views/interviews/macarthur.shtml
We Must Dismantle Our Democracy in Order to Save It
http://www.salon.com/comics/tomo/2001/10/01/tomo/
Muslim Leaders Struggle With Mixed Messages
http://www.washingtonpost.com/wp-dyn/articles/A55677-2001Oct1.html
the followers of John Adams are bringing back the Alien and Sedition Acts
http://www.salon.com/politics/feature/2001/10/03/ashcroft/print.html
conservative dupes learn what they really voted for
http://www.nytimes.com/2001/10/03/national/03WEST.html
Anti-Terrorism Bill Hits Snag on the Hill
http://www.washingtonpost.com/wp-dyn/articles/A61023-2001Oct2.html
Florida Task Force's Recommendation: Give State Police Added Power
http://www.gopbi.com/partners/pbpost/epaper/editions/tuesday/news_4.html
USACM letter regarding encryption controls
http://www.acm.org/usacm/crypto/gregg-crypto-letter.html
pro-Carnivore column employing several jargon techniques
http://writ.news.findlaw.com/commentary/20011001_hodes.html
Net Freedom Fears "Hurt Terror Fight"
http://news.bbc.co.uk/hi/english/uk_politics/newsid_1568000/1568254.stm
Detecting Steganographic Content on the Internet
http://www.citi.umich.edu/techreports/reports/citi-tr-01-11.pdf

Bill Introduced to Encourage Public-Private Information Sharing
http://www.gcn.com/vol1_no1/daily-updates/17197-1.html
documents relevant to Homeland Defense
http://stinet.dtic.mil/dticrev/vol5-number4.html
radio story and background article about new high-tech spy planes (when they fly over Afghanistan, it's a
war story; here, it's civil liberties)
http://www.npr.org/ramfiles/me/20011002.me.10.ram
http://www.fas.org/irp/program/collect/global_hawk.htm
Challenges for the Supreme Court in the Wake of Terrorism
http://writ.news.findlaw.com/lazarus/20011002.html
House Panel Approves Bill Expanding Surveillance
http://www.nytimes.com/2001/10/04/national/04RIGH.html
the anti-terrorism bill
http://www.house.gov/judiciary/hr2975terrorismbill.pdf
analysis of the bill
http://www.eff.org/Privacy/Surveillance/20011001_house_patriot_analysis.html
http://www.epic.org/privacy/terrorism/cong_ltr_10_02_01.html
argument against racial profiling in the investigation
http://www.law.com/cgi-bin/nwlink.cgi?ACG=ZZZWEVL1BSC
Senator Feinstein Urges Major Changes in US Student Visa Program
http://www.senate.gov/~feinstein/releases01/stvisas1.htm
Democracy in Wartime
http://www.nytimes.com/2001/10/03/opinion/03SCHL.html
Can the New York Times Count -- or Quote -- Peace Activists?
http://www.fair.org/activism/nyt-peace-activists.html
A Battle-Ready Net?
http://www.businessweek.com/technology/content/oct2001/tc2001101_7845.htm
What Went Wrong (with the CIA)

ISSN: 1575-2844 · DOI: http://dx.doi.org/10.15178/va.2001.29.1-14

http://newyorker.com/FACT/
Unscreened Ground Crews Add to Flying Jitters
http://www.latimes.com/news/printedition/california/la-000078980oct03.column
White House, Senate Reach Agreement on Anti-Terrorism Bill
http://www.latimes.com/news/printedition/asection/la-000079336oct04.story
Terror Laws Near Votes in House and Senate
http://www.nytimes.com/2001/10/05/national/05RIGH.html?pagewanted=print
Ashcroft Pushes Stronger Antiterrorism Bill
http://www.cnn.com/2001/US/10/04/inv.ashcroft.terrorism/
Toward a Balanced Terrorism Bill
http://www.nytimes.com/2001/10/04/opinion/04THU3.html
Proposed Legislation Significantly Affecting the Computer Profession
http://www.usenix.org/whatsnew/legislation.html
Consortium Responds to More Restrictive Access to Visas by Non-Immigrants
http://www.uciep.org/press1.htm
Report Warns of Rights Abuse Risk
http://www.latimes.com/news/printedition/asection/la-000079340oct04.story
Viisage Selected to Deploy the First Face-Recognition System in a US Airport
http://biz.yahoo.com/bw/011004/42302_1.html
Nixed "Holy War" Web Site Offered PGP Encryption Key
http://www.newsbytes.com/news/01/170828.html
Massive Search Reveals No Secret Code in Web Images
http://www.newscientist.com/news/news.jsp?id=ns99991340
Twenty Most Critical Internet Security Vulnerabilities
http://66.129.1.101/top20.htm
Securing the Lines of a Wired Nation
http://www.nytimes.com/2001/10/04/technology/circuits/04SECU.html
Immigrants' Driver's License Bill a Victim of Terrible Timing
http://www.latimes.com/news/printedition/california/la-000079422oct04.column

Muslim Leaders Condemn Thatcher Attack
http://www.guardian.co.uk/wtccrash/story/0,1300,563247,00.html
"in America, history shows, war does not override the calculus of politics"
http://www.theatlantic.com/unbound/polipro/pp2001-10-03.htm
Bill to Boost Defendants' Rights in Italy Hinders Terrorism War (Berlusconi and his cronies are changing
criminal law to protect themselves)
http://www.latimes.com/news/printedition/asection/la-000079343oct04.story
Senate Favors Federal Airport Screeners
http://www.latimes.com/news/printedition/asection/la-000079338oct04.story
Three Political Websites Downed After Government "Homeland Security" Threat
http://slash.autonomedia.org/article.pl?sid=01/09/30/1859212
Activists and Companies Confront Face Recognition Software
http://www.notbored.org/ciberpais2.html
Carnivore Substitute Keeps Feds Honest
http://www.theregister.co.uk/content/6/21992.html
New FTC Head Wants "Pause" in Push for Privacy Laws
http://www.computerworld.com/storyba/0,4125,NAV47_STO64453,00.html
http://www.nytimes.com/2001/10/03/technology/03PRIV.html
Zero-Knowledge Shelves Anonymity Tool (that sort of thing probably can't work unless it is built in)
http://news.cnet.com/news/0-1005-200-7412015.html
Seeking Sunlight for a Prisoner in the Chinese Gulag
http://www.latimes.com/news/opinion/commentary/la-000078572oct01.story
argument for a sunset clause in the anti-terrorism bill
http://www.theatlantic.com/politics/nj/taylor2001-10-02.htm
Do New Anti-Terrorism Proposals Pass Constitutional Muster?
http://www.law.com/cgi-bin/nwlink.cgi?ACG=ZZZKRW2IGSC
argument against Bush's proposals to restrict civil liberties

ISSN: 1575-2844 · DOI: http://dx.doi.org/10.15178/va.2001.29.1-14

http://prospect.org/print/V12/18/cole-d.html
The Terrorism Bill Does Too Much and Not Enough
http://www.tnr.com/101501/rosen101501.html
Leahy on "Protecting Constitutional Freedoms in the Face of Terrorism"
http://www.senate.gov/~leahy/press/200110/100301.html
text of the Senate's anti-terrorism bill
http://www.senate.gov/~leahy/press/200110/USA.pdf
http://www.senate.gov/~leahy/press/200110/100401a.html
Indefinite Detention Based Upon Suspicion Under the New Anti-Terrorism Act
http://writ.news.findlaw.com/commentary/20011005_ramasastry.html
Surveillance Warrants Keep Secret Court Busy
http://www.usatoday.com/usatonline/20011004/3508205s.htm
concerns about efforts to revise government controls on strong encryption
http://www.acm.org/usacm/crypto/crypto-controls-memo.html
overly-broad definition of "terrorism" in the Administration's proposal
http://www.acm.org/usacm/terrorist-memo.html
ACLU Calls New Senate Terrorism Bill Significantly Worse
http://www.aclu.org/safeandfree/
"Sunset Clause" Could Trip Up Anti-Terror Bill
http://www.latimes.com/news/printedition/asection/la-000079529oct05.story
Judge Strikes Down Parts of 1996 Terrorism Law
http://www.latimes.com/news/printedition/asection/la-000079527oct05.story
Paul Wolfowitz wants to replace Posse Comitatus (add up their proposals and you're well on the way to
martial law)
http://www.newsday.com/news/nationworld/nation/wire/sns-ap-attacks-defense-strategy1004oct04.story
Britain as a Cautionary Tale for a New Age of Surveillance

http://www.nytimes.com/2001/10/07/magazine/07SURVEILLANCE.html?pagewanted=all
Florida's Continued Alert Status Criticized
http://www.miami.com/herald/content/news/local/dade/digdocs/112393.htm
recommendations to help secure computing infrastructure against attacks
http://www.acm.org/usacm/crypto/comp-sec-memo.html
hard-to-evaluate claim that the hijackers used steganography
http://abcnews.go.com/sections/primetime/DailyNews/PRIMETIME_011004_steganography.html
The Supreme Court Returns to a Changed Legal Landscape
http://writ.news.findlaw.com/dorf/20011003.html
Censorship After 9/11: The Bill Maher "Coward" Comment
http://www.holtuncensored.com/members/column269.html
FBI testimony to the Senate about terrorist groups
http://www.fbi.gov/congress/congress01/freeh051001.htm
Senator Rethinks Stance on Students
http://www.latimes.com/news/printedition/asection/la-000079922oct06.story
FAA, Airlines Stalled Major Security Plans
http://www.latimes.com/news/nationworld/nation/la-100601air.story
Watchdog Sites Shut Down in Interest of National Security
http://newsfactor.com/perl/story/13990.html
Security Breaches Vary Widely at US Airports
http://www.cnn.com/2001/US/10/05/inv.airport.security/
Tighter Airport Security Is Just a Flight of Fancy
http://www.latimes.com/news/printedition/california/la-000079574oct05.column
criticism of UK's anti-terrorism legislation
http://www.magnacartaplus.org/bills/terrorism/index.htm
House Votes for More Spy Aid and to Pull in Reins on Inquiry
http://www.nytimes.com/2001/10/06/national/06INTE.html

ISSN: 1575-2844 · DOI: http://dx.doi.org/10.15178/va.2001.29.1-14

conservative support for the extreme provisions of the anti-terrorism bill
http://www.opinionjournal.com/extra/?id=95001279
http://www.latimes.com/news/printedition/suncommentary/la-000080099oct07.story
A High-Tech Home Front (including criticism of face recognition systems) (may not work under Netscape,
or Explorer either for that matter)
http://www.msnbc.com/news/635417.asp
National ID Cards: One Size Fits All
http://www.nytimes.com/2001/10/07/weekinreview/07WAKI.html
New Slogan in Washington: Watch What You Say ("a suspension of freedom unlike anything since World
War II")
http://www.nytimes.com/2001/10/07/national/07PRES.html
Demonizing Dissent
http://www.workingforchange.com/article.cfm?ItemID=12064
Now We Really Need Rights
http://www.observer.co.uk/comment/story/0,6903,564633,00.html

Jesús Cea Avió
njcea@hispasec.com

Copiado de la lista "noticias@hispasec.com" 09/10/2001