

CRYPTO-GRAM
15 febbraio 2008

Scritta da Bruce Schneier
Fondatore e CTO di BT Counterpane

Edizione italiana curata da Communication Valley SpA
<<http://www.communicationvalley.it/>>

CRYPTO-GRAM è una newsletter mensile gratuita che offre riassunti, analisi, approfondimenti, e commenti sulla sicurezza (informatica e in generale) e sulla crittografia.

Per consultare i numeri arretrati, o per iscriversi, andare all'indirizzo:
<<http://www.schneier.com/crypto-gram.html>>.

Oppure si può leggere il presente numero direttamente sul Web, all'indirizzo:
<<http://www.schneier.com/crypto-gram-0703.html>>.

Gli stessi articoli della newsletter sono disponibili sul blog di Bruce Schneier "Schneier on Security": <<http://www.schneier.com/blog>>.

Crypto-Gram è anche consultabile in formato RSS.

** *** ***** ***** ***** ***** ***** ***** ***** ***** *****

In questo numero:

- Sicurezza contro Privacy
- MySpace e i Procuratori Generali degli Stati Uniti contro i predatori sessuali
- Tecnologia anti-missilistica su aerei commerciali
- News
- Il lock-in
- Hacking ai danni delle reti energetiche
- Le news su Schneier/BT Counterpane
- Mujahideen Secrets 2
- News della TSA
- Il Dipartimento per la Sicurezza Nazionale mette in guardia sul pericolo di donne bombarole suicide
- Concedere la patente di guida a immigrati clandestini
- Commenti dei lettori

** *** ***** ***** ***** ***** ***** ***** ***** ***** *****

Sicurezza contro Privacy

Se esiste un dibattito che sintetizza la politica post-11 settembre, è quello della sicurezza contro la privacy. Quale delle due è più importante? A quanta privacy siete disposti a rinunciare per la sicurezza? E poi, ci possiamo davvero permettere la privacy

in quest'epoca di insicurezza? Sicurezza contro Privacy: è la battaglia del secolo, o almeno di questo primo decennio.

In un articolo del "New Yorker" del 21 gennaio Michael McConnell, direttore della National Intelligence, parla di un progetto proposto per monitorare tutte (proprio così, TUTTE) le comunicazioni Internet a fini di sicurezza. Un'idea talmente estrema che l'aggettivo "orwelliano" è un eufemismo.

Nell'articolo è contenuto questo passaggio: "Perché il cyberspazio possa essere controllato, l'attività in Internet dovrà essere rigorosamente monitorata. Ed Giorgio, che sta collaborando con McConnell al progetto, ha affermato che ciò significherebbe dare al governo l'autorità di esaminare il contenuto di ogni email, di ogni trasferimento di file o ricerca Web. 'Google possiede registri che potrebbero essere di grande aiuto in un'indagine cibernetica', ha detto. Giorgio avverte, 'Abbiamo un detto in questo mestiere: la privacy e la sicurezza sono un gioco a somma zero'".

Sono certo che abbiano quel detto nel loro mestiere. Ed è esattamente per questo che, quando un governo viene guidato da gente del loro mestiere, si converte in uno stato di polizia. Se la privacy e la sicurezza fossero davvero un gioco a somma zero, avremmo assistito a un'immigrazione di massa verso l'ex Germania dell'Est e verso la Cina di oggi. Se da un lato è vero che in stati di polizia come questi il crimine di strada è minore, nessuno ha dimostrato che i loro cittadini siano essenzialmente più sicuri.

Ci è stato detto che dobbiamo giungere a un compromesso fra sicurezza e privacy così tante volte (in dibattiti sulla sicurezza e sulla privacy, in concorsi di scrittura, sondaggi, articoli ragionati e retorica politica) che molti di noi non mettono nemmeno in discussione l'essenziale dicotomia.

Ma è una falsa dicotomia.

La sicurezza e la privacy non sono gli estremi opposti di un'altalena: non occorre accettare meno di una per ottenere di più dell'altra. Pensiamo a una serratura, a un allarme antirapina e a una recinzione molto alta. Pensiamo alle pistole, alle misure anti-contraffazione delle banconote e a quello stupido divieto sui liquidi negli aeroporti. La sicurezza influisce sulla privacy soltanto quando si basa sull'identità, ed esistono dei limiti a quel genere di approccio.

Dall'11 settembre, tre cose hanno potenzialmente aumentato la sicurezza aerea: l'irrobustimento dei portelli della cabina di pilotaggio, i passeggeri che hanno capito che devono reagire e, forse, la presenza di sky marshal. Tutto il resto, tutte le misure di sicurezza che vanno a intaccare la privacy, si tratta semplicemente di una messinscena di sicurezza e di uno spreco di risorse.

Analogamente, molte delle misure di "sicurezza" anti-privacy che oggi vediamo (documenti d'identità nazionale, intercettazioni senza mandati, data mining su larghissima scala, ecc.) fanno ben poco per migliorare la sicurezza, e in certi casi addirittura la compromettono. E le dichiarazioni di successo da parte del governo sono sbagliate oppure riguardano false minacce.

Il dibattito non è "sicurezza o privacy", ma "libertà o controllo".

Lo si può vedere nei commenti di funzionari del governo: "La privacy non deve più significare anonimato", sostiene Donald Kerr, vice direttore principale della national intelligence. "Invece, la privacy dovrebbe comportare che il governo e le imprese proteggano in modo adeguato le comunicazioni private delle persone e le loro informazioni finanziarie". Avete capito? Ci si aspetta da voi che rinunciate al controllo della vostra privacy per affidarlo ad altri, i quali, presumibilmente, finiscono col decidere quanta privacy meritate. Ecco che cos'è la perdita della libertà.

Non deve sorprendere che la gente preferisca la sicurezza alla privacy: 51% contro il 29% in un recente sondaggio. Anche se non vi identificate nella gerarchia di bisogni di Maslow, è ovvio che la sicurezza sia più importante. La sicurezza è cruciale per la sopravvivenza, non solo delle persone, ma di ogni essere vivente. La privacy è una caratteristica che riguarda solo gli esseri umani, ma è un bisogno sociale. È essenziale per la dignità personale, per la vita di famiglia, per la società, per ciò che ci rende umani, ma non per la sopravvivenza.

Se si imposta la falsa dicotomia, è naturale che le persone sceglieranno la sicurezza a scapito della privacy, soprattutto se prima le spaventiamo. Ma rimane una falsa dicotomia. Non esiste sicurezza senza privacy. E la libertà richiede sia sicurezza che privacy. La nota massima attribuita a Benjamin Franklin dice: "Chi è pronto a dar via le proprie libertà fondamentali per comprarsi briciole di sicurezza momentanea non merita né la libertà né la sicurezza". È anche vero che chi rinuncia alla privacy per la sicurezza finirà probabilmente senza l'una né l'altra.

L'articolo di McConnell sul "New Yorker":

<http://www.newyorker.com/reporting/2008/01/21/080121fa_fact_wright>

<<http://arstechnica.com/news.ars/post/20080117-us-intel-chief-wants-carte-blanche-to-peep-all-net-traffic.html>>

oppure <<http://tinyurl.com/2xkwvu>>

<<http://blog.wired.com/27bstroke6/2008/01/feds-must-exami.html>>

Giungere a compromessi fra sicurezza e privacy:

<http://www.huffingtonpost.com/ka-taipale/privacy-vs-security-se_b_71785.html>

oppure <<http://tinyurl.com/2gdqbn>>

<http://www.huffingtonpost.com/marc-rotenberg/privacy-vs-security-pr_b_71806.html>

oppure <<http://tinyurl.com/2hozm8>>

<http://findarticles.com/p/articles/mi_m0GER/is_2002_Winter/ai_97116472/pg_1>

oppure <<http://tinyurl.com/2yk23v>>

<http://www.rasmussenreports.com/public_content/politics/current_events/general_current_events/51_say_security_more_important_than_privacy>

oppure <<http://tinyurl.com/ypcen8>>

<<http://www.scu.edu/ethics/publications/briefings/privacy.html>>

<<http://www.csmonitor.com/2002/1015/p11s02-coop.html>>

Falsa dicotomia:

<<http://www.schneier.com/crypto-gram-0109a.html#8>>

<<http://www.wired.com/politics/law/commentary/circuitcourt/2006/05/70971>>

I commenti di Donald Kerr:

<http://www.schneier.com/blog/archives/2007/11/redefining_priv.html>

Articoli correlati:

<<http://www.schneier.com/essay-008.html>>
<<http://www.schneier.com/essay-096.html>>
<<http://www.schneier.com/essay-036.html>>
<<http://www.schneier.com/essay-160.html>>
<<http://www.schneier.com/essay-100.html>>
<<http://www.schneier.com/essay-108.html>>
<<http://www.schneier.com/essay-163.html>>
<<http://arstechnica.com/news.ars/post/20080119-analysis-metcalfes-law-real-id-more-crime-less-safety.html>>
oppure <<http://tinyurl.com/23h88d>>
<http://www.schneier.com/blog/archives/2007/09/more_on_the_ger_1.html>
<http://www.schneier.com/blog/archives/2007/06/portrait_of_the_1.html>
<http://www.schneier.com/blog/archives/2006/05/the_value_of_pr.html>

Questo articolo è originariamente apparso su Wired.com.

<http://www.wired.com/politics/security/commentary/securitymatters/2008/01/securitymatters_0124>
oppure <<http://tinyurl.com/yr98nf>>

** *** ***** ***** ***** ***** ***** ***** *****

MySpace e i Procuratori Generali degli Stati Uniti contro i predatori sessuali

MySpace ha raggiunto un accordo con i procuratori generali di 49 stati (Texas escluso) per proteggere i bambini da predatori sessuali presenti sul sito.

I procuratori generali stanno tutti congratulandosi fra loro, e naturalmente anche MySpace lo sta facendo, e vi sono parecchi commenti a riguardo. A me questo pare molto rumore per nulla.

Le contromisure non faranno nulla per fermare i predatori di bambini su MySpace. Del resto non è che esista un reale problema di predatori di bambini su MySpace, soltanto qualche storia eccessivamente pubblicizzata. È semplicemente una messinscena di sicurezza contro una minaccia da trama cinematografica. Ma noi esseri umani abbiamo un bias cognitivo assai radicato che ci fa sopravvalutare le minacce contro i nostri bambini, per cui il tutto ha un senso.

<<http://www.reuters.com/article/technology-media-telco-SP/idUSN1441132520080115>>
oppure <<http://tinyurl.com/28hunb>>
<<http://www.nytimes.com/2008/01/15/us/15myspace.html>>
<http://www.huffingtonpost.com/anastasia-goodstein/myspaces-missed-opportun_b_81637.html>
oppure <<http://tinyurl.com/yuyk8v>>
<http://www.informationweek.com/blog/main/archives/2008/01/myspace_child_p.html>
oppure <<http://tinyurl.com/294l9m>>
<http://www.news.com/8301-13577_3-9850057-36.html?tag=newsmag>

<<http://www.myfoxstl.com/myfox/pages/News/Detail?contentId=5485524&version=1&locale=EN-US&layoutCode=TSTY&pageId=3.2.1>>

oppure <<http://tinyurl.com/273hXu>>

<<http://www.techliberation.com/archives/043224.php>>

<<http://www.techcrunch.com/2008/01/14/what-does-myspaces-child-protection-deal-mean-for-facebook-bebo-and-google/>>

oppure <<http://tinyurl.com/3ba2sd>>

Dettagli delle contromisure:

<<http://ago.mo.gov/newsreleases/2008/pdf/MySpace-JointStatement0108.pdf>>

** *** ***** ***** ***** ***** ***** ***** ***** ***** *****

Tecnologia anti-missilistica su aerei commerciali

Si tratta di qualcosa che è già saltato fuori in precedenza, ma questa volta sembra proprio che si farà. Da MSNBC: "La tecnologia dovrebbe fermare un attacco missilistico rilevando il calore sprigionato dal missile e quindi emettendo un raggio laser che interferisca con il sistema di guida del missile".

Qualche mia impressione sull'argomento. Uno, è una messinscena di sicurezza contro una minaccia da trama cinematografica. Due, dando per assodato che sia vero, attaccare una scatola vuota sotto la fusoliera dell'aereo con la scritta "Sistema Laser Anti-Missilistico" potrebbe essere un deterrente altrettanto efficace a una frazione del costo. E tre, chi ci assicura che non stiano facendo proprio questo?

<<http://www.msnbc.msn.com/id/22507209/>>

<<http://blog.wired.com/27bstroke6/2008/01/dhs-testing-thr.html>>

Storie precedenti:

<http://www.schneier.com/blog/archives/2005/07/anti-missile_de.html>

<http://www.schneier.com/blog/archives/2006/08/antimissile_def.html>

Il post nel mio blog:

<http://www.schneier.com/blog/archives/2008/01/antimissile_tec.html>

** *** ***** ***** ***** ***** ***** ***** ***** ***** *****

News

Rapine in banca basate sull'ingegneria sociale nell'area di DC:

<<http://www.schneier.com/blog/archives/2008/01/socialengineeri.html>>

Un buon articolo su una nuova tendenza dello spionaggio aziendale: compagnie come Wal-Mart e Sears si sono ridotte a sorvegliare segretamente dipendenti, partner, giornalisti e persino utenti Internet per proteggersi da "minacce globali".

<<http://www.ciozone.com/index.php/Management/Wal-Mart-Spying-Good-Bad-Or-Just-The-Wave-Of-The-Futureu.html>>

oppure <<http://tinyurl.com/24pud9>>

Rudy Giuliani sulla sicurezza antiterrorismo:

<http://www.city-journal.org/2008/18_1_homeland_security.html>

<<http://padraic2112.wordpress.com/2008/01/17/why-rudy-giuliani-should-not-be-the-next-president-part-i/>>

<<http://padraic2112.wordpress.com/2008/01/18/why-rudy-giuliani-should-not-be-the-next-president-part-ii/>>

oppure <<http://tinyurl.com/23vzpc>>

Il "New York Times" scrive in merito a una connessione plausibile tra paura e malattia cardiaca.

<<http://www.nytimes.com/2008/01/15/science/15tier.html>>

Un quattordicenne ha modificato il telecomando di un televisore per scambiare treni su rotaia nella città polacca di Lodz. La lezione qui è che la sicurezza attraverso la segretezza, unita alla sicurezza fisica dell'attrezzatura, non sono state sufficienti. Questo ragazzino ha scavalcato ogni barriera e ha effettuato il reverse-engineering del protocollo del controllo a infrarossi. Poi ha potuto giocare ai trenini elettrici con treni veri e propri.

<http://www.theregister.co.uk/2008/01/11/tram_hack/>

<<http://www.cs.columbia.edu/~smb/blog/2008-01/2008-01-11.html>>

<<http://www.telegraph.co.uk/news/main.jhtml;jsessionid=Y5X3DLZOSFSAPQFIQMFSFFOAVCBQ0IV0?xml=/news/2008/01/11/wschooll11.xml>>

oppure <<http://tinyurl.com/3af8uh>>

Alla fine dell'Ottocento, le cassette degli allarmi antincendio venivano tenute sotto chiave per evitare falsi allarmi: questo aggravò il Grande Incendio di Chicago nel 1871. Ora paragonatelo con una proposta di legge a New York che obbligherà le persone a ottenere una licenza prima di poter acquistare rilevatori di attacchi chimici, biologici o radiologici.

<http://www.schneier.com/blog/archives/2008/01/locked_fire_box.html>

La tessera dei trasporti pubblici olandese, che è già costata al governo la cifra di 2 miliardi di dollari (no, non è un refuso), è stata hackerata ancor prima di essere messa in circolazione. Da un gruppo di studenti. Secondo me il sistema è stato progettato da persone che non comprendono la sicurezza, e che quindi hanno creduto fosse facile.

<<http://www.cs.vu.nl/~ast/ov-chip-card>>

<<http://www.freedom-to-tinker.com/?p=1250>>

Maggiori informazioni su SmartWater:

<http://www.schneier.com/blog/archives/2008/01/smartwater_work.html>

Nuovo dispositivo, che combina un taser e un lettore MP3. Pare che non sia uno scherzo.

<<http://www.guardian.co.uk/business/2008/jan/08/technology.gadgets>>

Non ho il benché minimo dubbio che vi saranno delle falle di sicurezza nei termostati controllabili da remoto, che permetteranno agli hacker di ottenerne il controllo. Fatelo in una giornata particolarmente calda, e potreste persino causare un grosso black-out.

<<http://www.nytimes.com/2008/01/11/us/11control.html?ex=1357707600&en=608b7b5bb2921934&ei=5088>>

oppure <<http://tinyurl.com/2f8cqs>>

La proposta è stata ritirata:

<<http://www.energy.ca.gov/title24/2008standards/faq.html>>

<<http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/01/17/BARNUGIKF.DTL>>

oppure <<http://tinyurl.com/yp6ft7>>

Ricompone via software documenti distrutti. Il contesto riguarda documenti della Stasi dell'ex Germania dell'Est stracciati e fatti a pezzi, ma la tecnologia è più generale.

<http://www.wired.com/politics/security/magazine/16-02/ff_stasi?currentPage=all>

oppure <<http://tinyurl.com/38talc>>

Una "storia del terrore" secondo cui persone non musulmane verrebbero reclutate come terroristi nel Regno Unito.

<http://www.schneier.com/blog/archives/2008/01/al_qaeda_recru.html>

Una pistola passa inosservata a un checkpoint della TSA in un aeroporto, e quando il proprietario notifica l'errore viene arrestato. E questo che diavolo dovrebbe insegnare?

<<http://www.cnn.com/2008/US/01/23/airport.gun/index.html>>

Continue battaglie nella Guerra all'Imprevisto:

Una valigia in Nuova Zelanda.

<<http://www.stuff.co.nz//4366917a11.html>>

Un cittadino americano che fotografa tutti i 50 campidogli statali.

<<http://www.nytimes.com/2008/01/20/arts/design/20shat.html>>

Piattaforma petrolifera in mare aperto evacuata dopo che qualcuno aveva sognato una bomba.

<<http://news.scotsman.com/scotland/Rig-worker39s-39dream39-sparked-bomb.3763123.jp>>

<<http://www.timesonline.co.uk/tol/news/uk/article3346196.ece>>

<<http://www.guardian.co.uk/uk/2008/feb/11/uksecurityandterrorism>>

<http://www.metro.co.uk/news/article.html?in_article_id=98289&in_page_id=34>

Lo Sheridan College in stato di contenimento preventivo perché qualcuno ha notato un treppiede.

<<http://video.msn.com/?mkt=en-ca&brand=sympatico&fg=rss&vid=1e18560e-eab4-4cd7-a1e3-d2e45e2f465f&from=37>>

<http://blogto.com/city/2008/02/tripod_prompts_lockdown_at_sheridan_college/>

<http://www1.sheridaninstitute.ca/corporate/news/2008/post_lockdown.cfm>

Un uomo arrestato perché in possesso di un lettore MP3.

<http://www.dailymail.co.uk/pages/live/articles/news/news.html?in_article_id=513875&in_page_id=1770>

Un aggiornamento sulle telecamere di sicurezza nella metropolitana di New York:

<<http://blog.wired.com/defense/2008/01/nycs-subway-spy.html>>

L'etica dei robot militari autosufficienti:

<<http://www.cc.gatech.edu/ai/robot-lab/online-publications/formalizationv35.pdf>>

Ricordate la "guerra cibernetica" dello scorso anno in Estonia? Quando qualcuno chiede un mio parere, in genere dico che la vicenda non è chiara e che forse si è trattato soltanto di ragazzi che hanno giocato alla politica. La realtà è ancora più banale: "...L'aggressore ... non si tratta di un membro dell'esercito russo, né di un guerriero cibernetico amareggiato che lavora per i servizi segreti di Putin. Non vive nemmeno in

Russia. È un cittadino [ventenne] estone di origine russa, infuriato per tutta quella faccenda della statua".

<<http://blog.wired.com/27bstroke6/2008/01/we-traced-the-c.html>>

Due etiopi, addetti alla pulizia della cabina, sono stati trovati mentre si nascondevano nel soffitto di un aereo dopo il suo atterraggio a Dulles. Presumibilmente fu permesso loro di salire a bordo ad Addis Abbaba, ma nessuno si è premurato di controllare se poi fossero scesi dall'aereo.

<<http://www.wusa9.com/news/local/story.aspx?storyid=67662>>

Articolo interessante sulle tecniche e procedure dei terroristi per evitare le intercettazioni:

<http://www.washingtonpost.com/wp-dyn/content/article/2008/01/04/AR2008010403573_pf.html>

Dati come inquinamento:

<http://www.schneier.com/blog/archives/2008/01/data_as_polluti.html>

L'FBI conosce l'identità degli autori del worm Storm?

<http://www.schneier.com/blog/archives/2008/01/fbi_knows_ident.html>

"Psychology Today" sulla valutazione dei rischi e sulla nostra incapacità nell'effettuarla:

<<http://www.psychologytoday.com/articles/pto-20071228-000005.html>>

Un documento illegalmente diffuso mostra come il governo britannico abbia intenzione di costringere i propri cittadini a essere inclusi in un database di identificazione nazionale.

<<http://www.boingboing.net/2008/01/29/leaked-uk-govt-doc-r.html>>

<http://craphound.com/NIS_Options_Analysis_Outcome.pdf>

Il governo bavarese vuole intercettare le chiamate effettuate con Skype_

<http://wikileaks.org/wiki/Bavarian_trojan_for_non-germans>

<<http://www.boingboing.net/2008/01/26/german-govt-caught-b.html>>

Rilevare armi nucleari sfruttando il network di telefonia cellulare. Non sono molto convinto sia una buona idea implementare un tale sistema, ma mi piace l'idea di attaccare una rete di sensori a livello nazionale in cima all'infrastruttura cellulare già esistente.

<<http://news.uns.purdue.edu/x/2008a/080122FischbachNuclear.html>>

Think Illegal Downloading Is Free? [Pensate che il download illegale sia gratuito?]

<<http://www.flickr.com/photos/68708714@N00/2219282175/sizes/l/>>

Provo sentimenti contrastanti sul fatto che la NSA tenga sotto controllo il traffico Internet del governo degli Stati Uniti, ma in generale penso che sia una buona idea.

<<http://www.washingtonpost.com/wp-dyn/content/article/2008/01/25/AR2008012503261.html>>

oppure <<http://tinyurl.com/2avcq2>>

In Svezia, persone di piccola statura si nascondono nei bagagli sugli autobus e rubano oggetti mentre i bagagli si trovano al deposito. Bizzarro, ma brillante.

<http://www.theregister.co.uk/2008/01/23/dwarf_coach_robberies/>

Il Dipartimento per la Sicurezza Nazionale sta finanziando il controllo di software open source affinché vengano rilevati bug di sicurezza e siano riparati. Scoprono in media una falla di sicurezza ogni mille righe di codice. E quando la falla viene tappata, la sicurezza di tutti migliora.

<http://www.informationweek.com/story/showArticle.jhtml?articleID=205600229&cid=RSSfeed_IWK_All>

oppure <<http://tinyurl.com/2gdbst>>

<http://www.pcworld.com/businesscenter/article/141226/open_source_security_bugs_uncovered.html>

oppure <<http://tinyurl.com/yqua3t>>

Il sistema fiscale a due livelli del Regno Unito: pessima sicurezza per tutti a eccezione dei ricchi e potenti:

<<http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2008/01/26/ntax126.xml>>

oppure <<http://tinyurl.com/2xamfq>>

Guasti ai cablaggi sottomarini nel Medio Oriente. Che sta succedendo?

<http://www.schneier.com/blog/archives/2008/02/fourth_undersea.html>

"Le 5 maggiori minacce di sicurezza del VoIP nel 2008": un bell'elenco di cose di cui preoccuparsi.

<<http://www.voip-news.com/feature/top-security-threats-2008-012408/>>

I criminali stanno utilizzando camion clonati per aggirare le misure di sicurezza:

<<http://abcnews.go.com/Blotter/story?id=4156618&page=1>>

Si tratta del medesimo problema delle uniformi fasulle, e del problema più generale delle false credenziali. È molto difficile da risolvere.

<http://www.schneier.com/blog/archives/2007/10/photo_id_requir_1.html>

<http://www.schneier.com/blog/archives/2006/01/forged_credenti.html>

Ecco un tizio che si mette una polo rossa e finge di essere un impiegato di Target così da poter rubare:

<<http://cbs4.com/local/target.fake.clerk.2.645377.html>>

Perché si crede che mettere agenti di polizia armati fino ai denti nelle stazioni della metropolitana di New York sia una buona idea? Che cosa si ottiene, a parte intimidire innocenti pendolari?

<<http://www.nytimes.com/2008/02/02/nyregion/02machinegun.html>>

Recentemente la Associated Press ha ottenuto centinaia di pagine di documenti relativi all'esercitazione "Cyber Storm" del 2006. La parte più interessante è quella in cui i partecipanti hanno attaccato i computer di gioco facendo infuriare gli arbitri.

<http://www.siliconvalley.com/security/ci_8126437>

<http://news.wired.com/dynamic/stories/C/CYBER_STORM?SITE=WIRE&SECTION=HOME&TEMPLATE=DEFAULT&CTIME=2008-01-31-07-38-13>

oppure <<http://tinyurl.com/3a4ffs>>

Cyber Storm: il rapporto.

<http://www.dhs.gov/xlibrary/assets/prep_cyberstormreport_sep06.pdf>

"The Onion" sul Terrore: "Tutti dobbiamo impegnarci a fare il possibile per preservare l'America tornando a concentrare le nostre priorità sulla contemplazione di minacce

letali, tremende forze invisibili che tramano per distruggerci nei modi più orripilanti. È soltanto attraverso la vigilanza e la determinazione di ogni patriota che possiamo mantenere quel senso di completo terrore che è essenziale per la continua esistenza di un'America prospera e tremante".

<http://www.theonion.com/content/opinion/we_must_all_do_our_part_to?utm_source=onion_rss_daily>

oppure <<http://tinyurl.com/23l3rj>>

Progressi nel riconoscimento facciale:

<http://www.schneier.com/blog/archives/2008/02/improvements_in.html>

Interessante riflessione di Nicholas Weaver su come la MPAA potrebbe far rispettare il copyright su Internet:

<<http://nweaver.blogspot.com/2008/01/security-thought-at-copyright-fighting.html>>

oppure <<http://tinyurl.com/2gmp8z>>

<<http://www.nnsquad.org/archives/nnsquad/msg00439.html>>

La dogana statunitense confisca i computer portatili in frontiera: se viaggiate all'estero, questo è importante:

<http://www.schneier.com/blog/archives/2008/02/us_customs_seiz.html>

Canon ha registrato un brevetto per l'aggiunta della scansione dell'iride del fotografo nei metadati delle fotografie, presumibilmente protetta da una firma digitale.

<<http://www.photographybay.com/2008/02/09/canon-iris-registration-watermark/>>

Il crittografo Stefan Brands ha una nuova azienda, Credentica, che permette alle persone di rivelare informazioni riservate mantenendo allo stesso tempo la privacy e riducendo la minaccia del furto di identità.

<<http://www.credentica.com/>>

<<http://www.wired.com/politics/security/news/2008/02/credentica>>

Conosco Stefan: è una persona in gamba. La crittografia che sta dietro a questo sistema è quasi certamente impeccabile. Mi piacciono sistemi come questo, e voglio che abbiano successo. Solo non vedo un business model realizzabile. Mi farebbe piacere essere smentito.

HotPlug consente di prendere e spostare un computer senza doverlo spegnere.

<<http://www.wiebetech.com/products/HotPlug.php>>

<http://www.youtube.com/watch?v=erq4TO_a3z8>

<<http://www.youtube.com/watch?v=-G8sEYCOv-o>>

Si veda anche MouseJiggler.

<<http://www.wiebetech.com/products/MouseJiggler.php>>

Il Dipartimento per la Sicurezza Nazionale in "The Onion." Divertente.

<http://www.theonion.com/content/news/dept_of_homeland_security_has>

** *** ***** ***** ***** ***** ***** ***** *****

Il lock-in

Acquistare un iPhone non è come comprare un'automobile o un tostapane. Il vostro iPhone comprende un complicato elenco di regole su ciò che potete e non potete fare con esso. Non potete installare applicazioni di terze parti non approvate. Non potete sbloccarlo e utilizzarlo con l'operatore di telefonia mobile che preferite. E Apple, con queste regole, fa sul serio: un aggiornamento software rilasciato nel settembre 2007 ha cancellato il software non autorizzato e, in alcuni casi, ha reso inutilizzabili gli iPhone craccati.

"Bricked" è il termine usato (letteralmente: "murato"), e Apple non si è scusata nemmeno un poco.

Le aziende di computer desiderano avere un controllo maggiore sui prodotti che vendono, e ricorrono a misure di sicurezza sempre più draconiane per ottenerlo. I motivi sono di natura economica.

Il controllo permette a una compagnia di limitare la concorrenza di prodotti ausiliari. Per i computer Macintosh, chiunque può commercializzare qualsiasi tipo di software. Ma nel caso dell'iPhone è Apple a decidere chi può produrre che cosa. Può incentivare la concorrenza quando vuole, e riservarsi una posizione di monopolio quando vuole. È può dettare termini e accordi a qualunque azienda voglia commercializzare prodotti e accessori per iPhone.

Ciò aumenta i profitti di Apple, ma il principale beneficio di tutto questo controllo, per Apple, è che aumenta il cosiddetto "lock-in". Il lock-in è un termine economico che definisce la difficoltà di passare a un analogo prodotto della concorrenza. Per alcuni prodotti, come la cola, non esiste lock-in. Oggi posso bermi una Coca-Cola e domani una Pepsi; nessun problema. Ma per altri prodotti è più difficile.

Passare a un altro word processor, per esempio, richiede l'installazione di un'applicazione nuova, l'apprendimento di una nuova interfaccia e di una nuova serie di comandi, la conversione di tutti i file (che potrebbero non convertirsi perfettamente) e del software personalizzato (che certamente richiederà un lavoro di riscrittura), e magari persino l'acquisto di nuovo hardware. Se la Coca-Cola smette di piacermi anche per un momento, cambierò prodotto: una lezione che la Coca-Cola ha imparato a caro prezzo nel 1985 quando modificò la formula e iniziò a mettere sul mercato la Nuova Coca-Cola. Ma il mio word processor deve farmi davvero imbestialire e per molto tempo prima che io possa solo considerare di imbarcarmi in tutto quel lavoro (e spese relative).

Il lock-in non è un fenomeno nuovo. È la ragione per cui i produttori di console di videogiochi fanno in modo che le cartucce per la propria console non funzionino su nessun'altra console, e questo permette loro di fissare un prezzo in perdita per le console e fare profitti vendendo i giochi. È la ragione per cui Microsoft non vuole mai aprire i propri formati in modo da essere letti da altre applicazioni. È la ragione per cui la musica comprata sull'iTunes Store per l'iPod non funzionerà su altre marche di lettori musicali. È la ragione per cui ogni operatore di telefonia mobile negli Stati Uniti si è opposto alla portabilità del numero di telefono. È la ragione per cui Facebook denuncia ogni azienda che cerca di ottenere i suoi dati e di metterli su siti Web concorrenziali. È ciò che sta alla base dei programmi frequent flyer delle compagnie aeree, delle tessere di fidelizzazione dei supermercati e del nuovo programma di Coca-Cola "My Coke Rewards".

Con un lock-in sufficiente, un'azienda può proteggere la sua quota di mercato anche se riduce il servizio al cliente, aumenta i prezzi, si rifiuta di innovare e in generale abusa della sua base di clienti. Non dovrebbe sorprendere il fatto che ciò assomigli più o meno a ogni esperienza che avete avuto con aziende del settore IT. Una volta che l'industria ha scoperto il lock-in, tutti hanno cercato di trovare il sistema per sfruttarlo il più possibile.

Gli economisti Carl Shapiro e Hal Varian hanno persino provato che il valore di una compagnia di software è il totale di lock-in. Questa è la logica: poniamo, per esempio, di avere 100 persone in un'azienda che utilizzano MS Office al costo di 500 dollari ciascuna. Se passare a Open Office costasse all'azienda meno di 50.000 dollari, lo farebbe. Se costasse più di 50.000 dollari, Microsoft aumenterebbe i prezzi.

Per la maggior parte, le aziende aumentano il proprio lock-in attraverso meccanismi di sicurezza. A volte sono i brevetti a preservare il lock-in, ma più spesso è la protezione anticopia, la gestione dei diritti digitali (DRM), il code signing o altri sistemi di sicurezza. Queste funzioni di sicurezza non sono ciò che siamo abituati a considerare sicurezza: non ci proteggono da una qualche minaccia esterna, bensì proteggono le aziende da NOI.

Microsoft ha pianificato per anni questo genere di meccanismo di sicurezza basato sul controllo. Prima chiamato Palladium e ora NGSCB (Next-Generation Secure Computing Base), l'idea di base è di costruire all'interno dell'hardware di un computer un sistema di sicurezza basato sul controllo. I dettagli sono complicati, ma i risultati variano dal limitare un computer al solo avvio da una copia autorizzata del sistema operativo, al proibire all'utente di accedere file "non autorizzati" o installare e utilizzare software non autorizzato. I vantaggi concorrenziali per Microsoft sono enormi.

Naturalmente, Microsoft non pubblicizza lo NGSCB in questi termini. L'azienda lo ha posizionato alla stregua di una misura di sicurezza, che protegge gli utenti da worm, Trojan e altro malware. Ma controllo non equivale a sicurezza, e questo genere di sicurezza basata sul controllo è estremamente difficile da realizzare nella giusta maniera; a volte ci rende più vulnerabili ad altre minacce. Forse è per questo motivo che Microsoft sta silenziosamente abbandonando lo sviluppo di NGSCB: abbiamo avuto BitLocker, e potremmo ottenere qualche altra funzionalità di sicurezza strada facendo, malgrado gli enormi investimenti fatti dai produttori di hardware quando hanno incorporato speciali hardware di sicurezza nelle loro schede logiche.

All'inizio del presente numero di Crypto-Gram ho parlato del dibattito sicurezza-privacy, e come in realtà si tratti di un dibattito nei termini di libertà contro il controllo. Qui vediamo in azione la stessa dinamica, ma in un contesto commerciale. Confondendo controllo e sicurezza, le aziende sono in grado di imporre misure di controllo che vanno contro i nostri interessi convincendoci che le stanno implementando per la nostra sicurezza.

Tornando ad Apple e all'iPhone, non so che cosa avranno intenzione di fare. Da una parte abbiamo questo rapporto di analisi che sostiene vi siano più di un milione di iPhone sbloccati, che costano ad Apple dai 300 ai 400 milioni di dollari di entrate. Dall'altra, Apple ha annunciato il rilascio di un software development kit per iPhone questo mese, eliminando la precedente restrizione e permettendo a produttori di terze parti di scrivere applicazioni per iPhone. Apple cercherà di mantenere il controllo

mediante una chiave di applicazione segreta che sarà richiesta per tutte le applicazioni di terze parti "ufficiali", ma ovviamente è già stata diffusa.

E il braccio di ferro della sicurezza continua...

Apple e iPhone:

<<http://www.nytimes.com/2007/09/29/technology/29iphone.html>>
<<http://www.bloomberg.com/apps/news?pid=20601087&sid=aWmqi08ZjbpM>>
<<http://www.engadget.com/2007/10/17/apple-planning-iphone-sdk-for-february/>>
oppure <<http://tinyurl.com/yvx5hr>>
<<http://www.engadget.com/2008/01/28/iphone-sdk-key-leaked/>>

Il libro di Shapiro e Varian:

<http://www.amazon.com/Information-Rules-Strategic-Network-Economy/dp/087584863X/ref=sr_1_1?ie=UTF8&s=books&qid=1202236504&sr=1-1>
oppure <<http://tinyurl.com/2eo23e>>

Microsoft e il Trusted Computing

<<http://schneier.com/crypto-gram-0208.html#1>>
<<http://www.cl.cam.ac.uk/~rja14/Papers/tcpa.pdf>>
<<http://www.microsoft.com/technet/archive/security/news/ngscb.msp>>
<http://www.schneier.com/blog/archives/2005/08/trusted_computi.html>

Commenti:

<<http://yro.slashdot.org/yro/08/02/07/2138201.shtml>>
<<http://stumble.kapowaz.net/post/25792347>>
<<http://www.kryogenix.org/days/2008/02/08/there-can-be-no-fud>>
<<http://girtby.net/archives/2008/2/8/vendor-lock-in>>

Questo articolo è precedentemente apparso su Wired.com.

<http://www.wired.com/politics/security/commentary/securitymatters/2008/02/securitymatters_0207>
oppure <<http://tinyurl.com/2mf82q>>

** *** ***** ***** ***** ***** ***** ***** *****

Hacking ai danni delle reti energetiche

La CIA ne ha sparata una grossa a una conferenza del SANS: "Mercoledì scorso a New Orleans, Tom Donahue, senior analyst della Central Intelligence Agency ha dichiarato di fronte a 300 tra funzionari dei governi degli Stati Uniti, Regno Unito, Canada e Olanda, e ingegneri e manager di sicurezza di industrie elettriche, idriche, petrolifere, del gas e di altre risorse critiche di tutto il Nord America, che 'Abbiamo informazioni, da varie regioni al di fuori degli Stati Uniti, in merito a intrusioni cibernetiche nelle infrastrutture dei servizi pubblici, seguite da richieste di denaro. Sospettiamo, ma non possiamo confermarlo, che alcuni di tali aggressori hanno avuto il vantaggio di possedere informazioni dall'interno. Abbiamo informazioni che attacchi cibernetici sono stati perpetrati al fine di mettere fuori uso centrali energetiche in varie regioni fuori degli Stati Uniti. In almeno un caso, l'interruzione ha provocato un black-out che ha colpito parecchi centri abitati. Non siamo a conoscenza di chi abbia eseguito tali attacchi, né

sappiamo il perché, ma il denominatore comune di tutti i casi sono state intrusioni via Internet”.

“Secondo il sig. Donahue, la CIA ha ponderato approfonditamente i rischi e i benefici della divulgazione di queste informazioni, e ha deciso per la trasparenza”.

E ci credo. Non vi è nulla di meglio che una voce di corridoio vaga e non circostanziata per evitare discussioni ragionevoli. Ma, naturalmente, tutti ne stanno comunque parlando e scrivendo.

Alan Paller del SANS è lieto di aggiungere qualche dettaglio. Da Forbes.com: “Negli ultimi due anni, gli hacker sono effettivamente riusciti a penetrare e a estorcere denaro a svariate compagnie che si servono di sistemi SCADA, afferma Alan Paller, direttore del SANS Institute, un’organizzazione che ospita un centro di crisi per aziende vittime di hacking. ‘Sono stati estorti centinaia di milioni di dollari, e forse più. È difficile saperlo, perché le compagnie pagano per mantenerlo un segreto’, sostiene Paller. ‘Questo genere di estorsione è la più grande storia non raccontata dell’industria del cybercrimine”.

E per aumentare il fattore paura: da “Information Week”: “La prospettiva di attacchi cibernetici mirati a danneggiare regioni densamente abitate pare aver spinto il governo a rendere pubbliche queste informazioni. Il problema, afferma Paller, ‘da un iniziale “dovremmo preoccuparci della questione” si è trasformato in “si tratta di una cosa che è necessario risolvere adesso”. Ecco perché, a mio avviso, il governo ha deciso di divulgarlo”.

Altre voci di corridoio da ibls.com: “Uno dei partecipanti al meeting ha detto che l’attacco non era molto conosciuto nell’industria, e molti sono rimasti sorpresi dalla notizia. La persona, che ha richiesto di rimanere anonima, ha detto: ‘Pare che vi siano stati un paio di incidenti in cui i ricattatori hanno interrotto l’erogazione di energia elettrica a parecchie città impiegando una specie di attacco ai danni della rete elettrica, e sembra non si sia trattato di un attacco di tipo fisico”.

E ancora un’iperbole da parte di qualcuno all’interno dell’industria. Dal Washington Post: “Negli ultimi 12-18 mesi vi è stato ‘un grande aumento di attacchi mirati alle nostre infrastrutture nazionali, [...] e si sono originati al di fuori degli Stati Uniti’, ha affermato Ralph Logan, titolare del Logan Group, una impresa di sicurezza cibernetica.

“È difficile rintracciare le fonti di tali attacchi, poiché solitamente vengono eseguiti da individui che si sono nascosti propagandosi in tre o quattro diverse reti di computer, ha detto Logan. Egli ritiene che gli attacchi siano stati lanciati da computer appartenenti a governi o eserciti stranieri, non da gruppi terroristici”.

Sono molto scettico a riguardo. Certamente, a parte finti attacchi simulati, esistono rischi piuttosto seri legati ai sistemi SCADA (Ganesh Devarajan ha tenuto una lezione all’ultimo DefCon su certi potenziali vettori di attacco), però a questo punto credo si tratti più di una minaccia futura che non un pericolo attuale. Ma questa notizia comunicata dalla CIA non ci dice nulla su come siano stati eseguiti gli attacchi. Erano contro sistemi SCADA? Erano contro workstation generiche, magari macchine Windows? È possibile che siano stati coinvolti dipendenti dall’interno, per cui si è davvero trattato di una vulnerabilità di sicurezza informatica? Non abbiamo idea.

L'estorsione cibernetica è indubbiamente in aumento: lo possiamo vedere a Counterpane. Avviene soprattutto ai danni di industrie marginali quali il gioco d'azzardo online, la pornografia online, ecc., che operano offshore in paesi come le Bermuda e le Isole Cayman. Si sta diffondendo maggiormente verso canali principali, ma questa è la prima volta che ho sentito che abbia preso di mira le aziende di energia elettrica. Certamente possibile, ma fa parte della voce messa in circolazione dalla CIA o è un dettaglio appiccicato in un secondo momento?

E la Wikipedia ha un elenco dei black-out. Quali sono stati provocati da hacker? Qualche informazione in più non sarebbe male, prima di farsi prendere dal panico.

La citazione dal SANS:

<<http://www.sans.org/newsletters/newsbites/newsbites.php?vol=10&issue=5>>

Articoli di cronaca:

<<http://www.engadget.com/2008/01/19/hackers-reportedly-targeting-cities-power-systems/>>

oppure <<http://tinyurl.com/35jlap>>

<http://www.forbes.com/2008/01/18/cyber-attack-utilities-tech-intel-cx_ag_0118attack.html>

oppure <<http://tinyurl.com/344t3w>>

<http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=1963>

oppure <<http://tinyurl.com/ypo8fz>>

<<http://www.informationweek.com/news/showArticle.jhtml?articleID=205901631>>

oppure <<http://tinyurl.com/34r575>>

<<http://www.washingtonpost.com/wp-dyn/content/article/2008/01/18/AR2008011803277.html>>

oppure <<http://tinyurl.com/2dd3lv>>

<<http://www.pcworld.com/article/id,141564-c,hackers/article.html>>

<http://www.forbes.com/2008/01/18/cyber-attack-utilities-tech-intel-cx_ag_0118attack.html>

oppure <<http://tinyurl.com/344t3w>>

<<http://it.slashdot.org/article.pl?sid=08/01/19/0138209>>

Un attacco SCADA simulato:

<http://www.schneier.com/blog/archives/2007/10/staged_attack_c.html>

L'intervento di Devarajan al DefCon:

<<http://www.defcon.org/html/defcon-15/dc-15-speakers.html#Devarajan>>

L'elenco di black-out presente nella Wikipedia:

<http://en.wikipedia.org/wiki/List_of_power_outages>

** *** ***** ***** ***** ***** ***** *****

Le news su Schneier/BT Counterpane

Un'intervista a Schneier:

<<http://searchsecurity.techtargget.com.au/topics/article.asp?DocID=1283751>>

oppure <<http://tinyurl.com/2aj9jw>>

A Schneier è stato consegnato il Norbert Wiener Award dai Computer Professionals for Social Responsibility (Professionisti informatici per la responsabilità sociale):
<<http://www.cpsr.org/news/press/wiener2008>>

Schneier ha tenuto il keynote a Linux.conf.au.

Un articolo sull'intervento:

<<http://www.itnews.com.au/News/69146,information-is-our-only-security-weapon-bruce-schneier.aspx>>

oppure <<http://tinyurl.com/387yyn>>

Filmato dell'intervento:

<<http://linux.conf.au/programme/presentations>>

<<http://mirror.linux.org.au/pub/linux.conf.au/2008/Wed/mel8-305.ogg>>

<<http://mirror.linux.org.au/pub/linux.conf.au/2008/Wed/mel8-305.spx>>

La successiva sessione di domande e risposte:

<<http://www.itwire.com/content/view/16422/1090/>>

** *** ***** ***** ***** ***** ***** ***** *****

Mujahideen Secrets 2

Mujahideen Secrets 2 è la nuova versione di uno strumento di criptatura che si dice sia stato scritto per aiutare i membri di Al Qaeda a criptare i segreti durante le loro comunicazioni via Internet.

Un certo numero di siti Web ne ha parlato, e nei vari articoli sono anche citati un paio di ricercatori di sicurezza. Ma leggendo estratti come questo, da "Computerworld", uno si domanda se queste persone abbiano una benché minima idea di ciò di cui stanno parlando: "Secondo Henry, da un punto di vista crittografico, Mujahideen Secrets 2 è un software davvero affascinante. Egli ha affermato che questo nuovo strumento è molto semplice da utilizzare e offre una crittografia a 2048 bit, un passo in avanti rispetto alla crittografia AES a 256 bit supportata nella versione originale".

Nessuno ha spiegato perché un terrorista dovrebbe fare uso di tale software e non di PGP; forse perché non si fidano di niente che provenga da un'azienda americana. Ma onestamente, non vedo dove sia l'eccezionalità: sono ormai quindici anni che esiste software di crittografia forte, molto economico se non addirittura freeware. E la NSA probabilmente decifra la maggior parte del materiale indovinando le password. A meno che l'intero programma non sia stato introdotto dalla stessa NSA, naturalmente.

La mia domanda è questa: gli articoli sostengono che il programma si serve di svariati algoritmi, fra cui RSA e AES. Utilizza Blowfish o Twofish?

<<http://www.networkworld.com/news/2008/020108-al-qaeda-encryption.html>>

<<http://www.networkworld.com/news/2008/012308-al-qaeda-encryption-security.html>>

oppure <<http://tinyurl.com/2g3lju>>

<<http://www.techworld.com/security/features/index.cfm?featureID=3950&pagtype=all>>

>

oppure <<http://tinyurl.com/22rwdf>>

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyId=16&articleId=9058619&intsrc=hm_topic>
oppure <<http://tinyurl.com/ypzpuo>>
<<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9060939>>
oppure <<http://tinyurl.com/2cf9nu>>
<<http://www2.csoonline.com/exclusives/column.html?CID=33516>>
<http://blogs.csoonline.com/a_gift_from_the_islamic_faithful_network_mujahedeen_secrets_2_program>
oppure <<http://tinyurl.com/3dn7ja>>
<<http://www.informationweek.com/internet/showArticle.jhtml?articleID=205918296>>
oppure <<http://tinyurl.com/yv34um>>

Il mio articolo su PGP:

<<http://www.schneier.com/essay-199.html>>

Il mio articolo sul password guessing:

<<http://www.schneier.com/essay-148.html>>

** *** ***** ***** ***** ***** ***** ***** *****

News della TSA

La TSA sta controllando i documenti di identità con maggiore attenzione, a caccia di contraffazioni: "Più di 40 passeggeri sono stati arrestati dallo scorso giugno in avanti, in casi in cui gli screener della TSA hanno rilevato passaporti modificati, visti e tessere di residenza fraudolenti, e patenti di guida contraffatte. Molti di quei passeggeri sono stati arrestati con accuse di immigrazione clandestina". I controlli dei documenti d'identità non hanno nulla a che vedere con la sicurezza aeroportuale. E anche se fosse, chiunque può volare con documenti falsi. E far rispettare le leggi sull'immigrazione non è compito della TSA.

<http://www.usatoday.com/news/nation/2008-01-20-blacklights_N.htm?csp=34>

Leggete questo estratto dal sito della TSA: "Controlliamo ogni passeggero; controlliamo ogni valigia in modo che i vostri ricordi siano del luogo in cui siete stati, non come ci siete arrivati. Siamo qui per fare in modo che i vostri piani di viaggio siano il più possibile piacevoli e privi di stress. Per favore, dedicate qualche istante del vostro tempo per familiarizzare con alcune delle nostre misure di sicurezza, così da poter risparmiare tempo una volta giunti in aeroporto". So che non lo intendono in questo modo, ma non vi pare che il messaggio suoni come "Sappiamo che non serve a nulla, ma potrebbe farvi sentire meglio"?

<<http://www.tsa.gov/travelers/airtravel/index.shtm>>

E perché è una novità quando un test rompe la sicurezza della TSA?

<<http://www.cnn.com/2008/US/01/28/tsa.bombtest/index.html>>

"Confessioni di un agente della TSA": alcuni sostengono si tratti di una bufala:

<<http://information.travel.aol.com/article/air/a/confessions-of-a-tsa-agent/20080123105909990002>>

oppure <<http://tinyurl.com/2ygsjh>>

Non ho idea del perché Kip Hawley si sorprenda che per i cittadini americani la TSA è sgradita quanto l'IRS (l'Agenzia delle Entrate USA).

<<http://www.theaviationnation.com/2007/12/30/tsa-leaked-memo-reveals-frustrated-chiefs/>>

oppure <<http://tinyurl.com/yr3rwy>>

La TSA ha un blog:

<<http://www.tsa.gov/blog>>

<<http://blog.wired.com/27bstroke6/2008/01/tsa-launches-bl.html>>

<<http://arstechnica.com/news.ars/post/20080131-tsa-blog-smackdown-explain-to-me-about-bomb-juice.html>>

oppure <<http://tinyurl.com/2fldwo>>

<<http://it.slashdot.org/it/08/02/01/2152216.shtml>>

<<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9060458>>

oppure <<http://tinyurl.com/26rajb>>

Io compaio perfino nell'elenco dei link.

** *** ***** ***** ***** ***** ***** ***** *****

Il Dipartimento per la Sicurezza Nazionale mette in guardia sul pericolo di donne bombarole suicide

Primo paragrafo: "I terroristi tendono sempre più a utilizzare donne come bombaroli suicidi per ostacolare la sicurezza e attirare attenzione sulle loro cause, conclude una valutazione dell'FBI e del Dipartimento per la Sicurezza Nazionale".

Didascalia della foto: "Le donne bombarole suicide possono servirsi di dispositivi che le facciano apparire gravide, afferma una valutazione di sicurezza".

Secondo paragrafo: "Nella valutazione viene detto che le agenzie 'non hanno dati di intelligence specifici o credibili che possano indicare che le organizzazioni terroristiche intendano servirsi di donne bombarole suicide contro bersagli all'interno dei loro paesi d'origine'".

Ma il Dipartimento per la Sicurezza Nazionale ci prende tutti per idioti o cosa?

<<http://edition.cnn.com/2008/US/02/12/suicide.bombers/index.html>>

** *** ***** ***** ***** ***** ***** ***** *****

Concedere la patente di guida a immigrati clandestini

Molti sostengono che dare la possibilità a immigrati clandestini di ottenere patenti di guida statali li aiuti e li incentivi a rimanere in questo paese illegalmente. Mike Cox, procuratore generale dello stato del Michigan, sul finire dello scorso anno ha emanato un'opinione secondo cui le patenti di guida avrebbero potuto essere concesse soltanto a

residenti statali in regola, e definendola "un altro strumento in più nella nostra iniziativa di sostegno della sicurezza dei documenti e di confine dello stato del Michigan".

In realtà saremmo una nazione più sicura se concedessimo patenti di guida e/o carte d'identità statali a qualsiasi residente ne facesse richiesta, a prescindere dal suo status di immigrazione. Concederle non ci rende meno sicuri, e rifiutarle ci espone a rischi maggiori.

I database delle patenti di guida emesse dai vari stati sono gli unici database esaustivi sui cittadini residenti negli Stati Uniti. Sono più completi e contengono più informazioni (fra cui fotografie e, in alcuni casi, impronte digitali), del database dell'Agenzia delle Entrate (IRS), del database della Previdenza Sociale, o dei database degli uffici anagrafe statali. Pertanto rappresentano uno strumento assai prezioso nelle mani della polizia: per investigare reati, rintracciare i sospettati e provarne la colpevolezza.

Eliminare gli 8-15 milioni di immigrati clandestini da questi database non farebbe altro che ostacolare l'operato delle forze dell'ordine. Naturalmente, chi non ottiene la patente non è che farà i bagagli e se ne andrà: continuerà a guidare senza patente, aumentando i premi assicurativi per tutti. Gli immigrati clandestini utilizzeranno documenti falsi, compreranno documenti veri da impiegati corrotti della Motorizzazione Civile (come fecero molti dei terroristi dell'11 settembre), falsificheranno i "breeder document" per ottenere documenti d'identità veri (un altro espediente dei terroristi dell'11 settembre), o ricorreranno al furto di identità. Questi milioni di persone continueranno a vivere e a lavorare negli Stati Uniti, invisibili a qualsiasi database governativo e quindi alla polizia.

Assumere che negare le patenti di guida ai clandestini sia un sistema per indurli ad abbandonare il paese è pensare con la testa nella sabbia.

Naturalmente, anche il solo tentativo di negare le patenti agli immigrati clandestini mette gli impiegati della Motorizzazione in una posizione impossibile, quella di verificare lo status di immigrazione. È un'operazione costosa in termini di tempo e denaro; e in più non funzionerà. La legge è complicata, e possono essere necessarie ore di lavoro per verificare lo status di immigrazione, per poi magari commettere lo stesso un errore. Gli incartamenti sono facili da falsificare, molto più facili delle stesse patenti di guida, e ciò significa che molti immigrati clandestini otterranno queste patenti che ora "proveranno" il loro status d'immigrazione.

E dall'altra parte, a un numero sempre maggiore di immigrati legali le patenti di guida verranno negate per errore; questo darà origine a cause legali e a spese governative extra.

Alcuni stati hanno preso in considerazione un sistema di patenti a livelli, che indichi esplicitamente lo status di immigrazione sulle patenti stesse. Ovviamente, neanche questo potrà funzionare. Gli immigrati clandestini preferiscono rischiare la cattura che ammettere il loro status di immigrazione di fronte alla Motorizzazione Civile.

Siamo tutti più sicuri se ognuno nella società si fida e rispetta le forze dell'ordine. Una società in cui gli immigrati clandestini hanno paura a parlare con la polizia perché temono di essere deportati è una società in cui sempre meno persone si fanno avanti per riferire reati, collaborare nelle indagini di polizia, e testimoniare in tribunale.

E infine, negare le patenti di guida agli immigrati clandestini non ci proteggerà dal terrorismo. Contrariamente a quanto si crede, non è necessario avere una patente di guida per imbarcarsi su un aereo. È possibile utilizzare un qualsiasi documento con foto emesso da un governo, quindi anche un passaporto straniero. E se si ha voglia di essere sottoposti a ulteriore screening, ci si può imbarcare anche senza documenti di identità. Questo è probabilmente il sistema utilizzato con successo da tutti coloro il cui nome si trova sulla no-fly list.

Un rapporto del 2003 dell'American Association of Motor Vehicle Administrators conclude: "Le immagini digitali delle patenti di guida sono state di enorme aiuto alle agenzie che si occupano della sicurezza nazionale. I 19 terroristi (dell'11 settembre) ottennero patenti di guida da diversi stati, e le autorità federali si sono appoggiate in maniera sostanziale su queste immagini per l'identificazione degli individui responsabili".

Che si tratti del Dipartimento per la Sicurezza Nazionale che cerca di proteggere il paese dal terrorismo, o le forze dell'ordine a livello locale, statale o nazionale che cercano di proteggere il paese dal crimine, saremmo tutti più al sicuro se invitassimo ogni persona adulta in America a ottenere una patente di guida.

Questo editoriale di opinione è apparso nella Detroit Free Press.
<<http://www.schneier.com/essay-205.html>>

** *** ***** ***** ***** ***** ***** ***** ***** ***** *****

Commenti dei lettori

Su questi argomenti vi sono centinaia di commenti nel mio blog, molti davvero interessanti. Cercate l'argomento sul quale intendete dare la vostra opinione, e unitevi al dibattito.

<<http://www.schneier.com/blog>>

** *** ***** ***** ***** ***** ***** ***** ***** ***** *****

CRYPTO-GRAM è una newsletter mensile gratuita che offre riassunti, analisi, approfondimenti, e commenti sulla sicurezza (informatica e in generale) e sulla crittografia. I numeri arretrati sono disponibili all'indirizzo <<http://www.schneier.com/crypto-gram.html>>. Per iscriversi, cancellare l'iscrizione o cambiare il proprio indirizzo a cui recapitare la newsletter, visitate sempre <<http://www.schneier.com/crypto-gram.html>>

La versione italiana è curata da Communication Valley SpA
<<http://www.communicationvalley.it/>>

Per iscriversi o cancellarsi andare all'indirizzo <<http://www.cryptogram.it/>>

I numeri arretrati sono disponibili all'indirizzo <<http://www.cryptogram.it/>>

Per informazioni <crypto-gram@communicationvalley.it>

I commenti a CRYPTO-GRAM devono essere inviati a schneier@counterpane.com. Si sottintende il permesso di riprodurre tali commenti, salvo indicazione contraria. I commenti possono venire adattati per ragioni di spazio e di chiarezza.

Inoltrate liberamente CRYPTO-GRAM a colleghi ed amici che possano trovare questa pubblicazione di un certo interesse. Viene concessa l'autorizzazione a ristampare CRYPTO-GRAM, a condizione che sia stampata integralmente.

CRYPTO-GRAM è realizzata da Bruce Schneier. Schneier è l'autore dei best seller "Beyond Fear", "Secrets and Lies" [tradotto in Italia col titolo "Sicurezza Digitale"] e "Applied Cryptography", e inventore degli algoritmi Blowfish, Twofish e Yarrow. È il fondatore e CTO di BT Counterpane e membro del comitato consultivo dell'Electronic Privacy Information Center (EPIC). Frequentemente scrive e partecipa a conferenze sulla sicurezza informatica e sulla crittografia. Il suo sito Web è all'indirizzo <<http://www.schneier.com>>.

BT Counterpane è leader mondiale nella protezione delle informazioni su network - l'inventore del Managed Security Monitoring gestito in outsourcing e la principale autorità nella riduzione efficace delle nuove minacce in ambito IT. BT Counterpane protegge reti per conto di governi e di aziende inserite nella Fortune 1000 a livello mondiale.

<<http://www.counterpane.com>>

Crypto-Gram è una newsletter personale. Le opinioni qui espresse non sono necessariamente quelle di BT o di BT Counterpane.

Copyright (c) 2008 - Bruce Schneier.