

CRYPTO-GRAM  
15 aprile 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:

- Terza edizione del concorso "Minaccia da Trama Cinematografica"
- L'impostazione mentale di chi si occupa di sicurezza
- News
- Percezione e realtà della sicurezza
- Intrappolamento Web
- Le news su Schneier/BT Counterpane
- Autovelox e conflitti di interessi
- Cinture di sicurezza e comportamento compensativo
- Internet e la censura
- Commenti dei lettori

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

Terza edizione del concorso "Minaccia da Trama Cinematografica"

L'obiettivo di questa terza edizione del concorso è creare paura. Non un terrore generico, ma una paura che si può attenuare grazie alla vendita del vostro nuovo prodotto. Esistono parecchi rischi là fuori, alcuni molto seri, altri talmente improbabili che non dovremmo neanche preoccuparci, altri ancora completamente inventati. Ed esistono svariati prodotti che forniscono sicurezza contro tali rischi.

Il vostro compito è inventarne uno. Prima di tutto, trovate un rischio o createne uno. Può essere una minaccia terroristica o criminale, il pericolo di una calamità naturale, o

un semplice rischio domestico, qualunque cosa. Più è bizzarro, meglio è. Poi create un prodotto che tutti DEVONO comprare per forza se vogliono proteggersi da tale minaccia. E infine scrivete un annuncio pubblicitario per quel prodotto.

Ecco un esempio, tratto da pagina 25 del catalogo Skymall - Primavera 2008 che sto sfogliando in aereo mentre scrivo questo pezzo:

“Una tartaruga è al sicuro in acqua, ma un bambino no! Anche quando viene sorvegliato con attenzione, un bambino può sparire sott’acqua nel giro di pochi secondi e ci si può accorgere della sua mancanza soltanto quando è troppo tardi. Il nostro nuovo sistema di allarme wireless da piscina è un must per chi possiede una piscina e per chi ha figli piccoli. Il braccialetto Turtle Wristband si blocca sul polso del bambino (è necessaria una chiave speciale per toglierlo) e rileva istantaneamente l’immersione in acqua, innescando un allarme molto acuto alla base wireless situata in casa o nel raggio di 30 metri dalla piscina, stazione termale o vasca da giardino. Tenete a portata di mano altri braccialetti per gli ospiti o per proteggere il vostro cane”.

Ogni proposta ha un limite di 150 parole (l’esempio citato era di 97 parole), perché la paura non richiede molte parole di spiegazione. Diteci perché dovremmo avere paura e perché dovremmo acquistare il vostro prodotto.

Le proposte verranno giudicate in base alla creatività, all’originalità, alla capacità di persuasione e alla plausibilità. Se il prodotto che inventate non esiste, va bene, ma ricordate che non si tratta di un concorso di fantascienza.

Rilevatori portatili di salmonella da usare nei bar e nelle insalaterie. Dispositivi acustici per stimare la vicinanza di una tigre in base alla forza del ruggito. Portafogli dotati di GPS da usarsi quando si viene derubati. Braccialetti che emettono un DNA fasullo per depistare i rilevatori di DNA. Il calmante quantico. La paura offre infinite opportunità di business. Buona fortuna.

Scadenza del concorso: 1 maggio. Pubblicate le vostre proposte in coda al post sul mio blog. E anche se non volete partecipare, andate a leggere quel che hanno prodotto gli altri. Siete dei lettori tremendamente creativi.

Il post sul blog:

Blog post:

<[http://www.schneier.com/blog/archives/2008/04/third\\_annual\\_mo.html](http://www.schneier.com/blog/archives/2008/04/third_annual_mo.html)>

Le regole del primo concorso “Minaccia da Trama Cinematografica”:

<[http://www.schneier.com/blog/archives/2006/04/announcing\\_movi.html](http://www.schneier.com/blog/archives/2006/04/announcing_movi.html)>

E i vincitori:

<[http://www.schneier.com/blog/archives/2006/06/movieplot\\_threa\\_1.html](http://www.schneier.com/blog/archives/2006/06/movieplot_threa_1.html)>

Le regole del secondo concorso “Minaccia da Trama Cinematografica”:

<[http://www.schneier.com/blog/archives/2007/04/announcing\\_seco.html](http://www.schneier.com/blog/archives/2007/04/announcing_seco.html)>

I semifinalisti:

<[http://www.schneier.com/blog/archives/2007/06/second\\_annual\\_m.html](http://www.schneier.com/blog/archives/2007/06/second_annual_m.html)>

E i vincitori:

<[http://www.schneier.com/blog/archives/2007/06/second\\_movieplo.html](http://www.schneier.com/blog/archives/2007/06/second_movieplo.html)>

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

L'impostazione mentale di chi si occupa di sicurezza

Uncle Milton Industries vende formicai per bambini dal 1956. Ricordo di averne aperto uno con un amico, anni fa. Nella confezione non erano incluse le formiche vere. Vi era invece una cartolina da compilare: si scriveva il proprio indirizzo e l'azienda vi avrebbe spedito un po' di formiche. Il mio amico fu sorpreso dal fatto che si potessero ricevere per posta delle vere formiche.

Io risposi: "Quel che è davvero interessante è che queste persone spediranno un tubo di formiche vive a qualsiasi indirizzo gli fornirai".

La sicurezza richiede una certa impostazione mentale. I professionisti di sicurezza, quelli bravi almeno, vedono il mondo con occhi diversi. Non possono entrare in un negozio senza pensare a come potrebbero rubare impunemente. Non possono utilizzare un computer senza chiedersi quali siano le vulnerabilità di sicurezza. Non possono andare a votare senza cercare di capire come fare a votare due volte. È semplicemente più forte di loro.

SmartWater è un liquido con un identificatore unico legato a un solo proprietario. Appena venni a conoscenza dell'idea scrissi: "Io lo utilizzerei sui miei oggetti di valore, come prova di possesso". E poi: "Credo che un'idea migliore sarebbe quella di spruzzarlo sui TUOI oggetti di valore, e poi chiamare la polizia".

Davvero, è più forte di noi.

Questo modo di ragionare non risulta naturale per la maggioranza delle persone. Non è naturale per gli ingegneri, per esempio. Un buon lavoro di ingegneria comporta il pensare a come fare in modo che le cose funzionino; l'impostazione mentale della sicurezza comporta il pensare a come fare in modo che le cose vadano male, si guastino, entrino in uno stato di errore. Comporta il ragionare come un aggressore, un avversario o un criminale. Non è che si debbano sfruttare le vulnerabilità trovate, ma se non si vede il mondo in questa maniera, non si potranno notare la maggior parte dei problemi di sicurezza.

Spesso ho riflettuto su quanto di questo possa essere una capacità innata e quanto sia insegnabile. In generale credo si tratti di un modo particolare di osservare il mondo, e che sia molto più semplice insegnare determinate esperienze di settore (crittografia, sicurezza del software, scassinare casseforti, falsificare documenti, ecc.) che non insegnare a qualcuno l'impostazione mentale della sicurezza.

Ed è per questo che è così interessante osservare il CSE 484, un corso di sicurezza informatica tenuto all'Università di Washington questo trimestre. Il professor Tadayoshi Kohno cerca di insegnare l'abito mentale di chi si occupa di sicurezza.

Potete vederne i risultati nel blog gestito dagli studenti, i quali vengono incoraggiati a scrivere recensioni sulla sicurezza dei prodotti più vari: confezioni di pillole, sistemi Quiet Care Elder Care per assistere gli anziani, Time Capsule di Apple, OnStar di GM, semafori, cassette di sicurezza e la sicurezza degli alloggi per studenti.

Uno dei casi più recenti trattati nel loro blog riguarda un rivenditore autorizzato di automobili. L'autore della recensione ha raccontato di come sia stato in grado di ritirare la sua auto semplicemente comunicando il proprio cognome all'addetto. Ora, qualunque proprietario di un'auto sarebbe felice di sapere quanto sia facile riprendersi la macchina, ma la prima cosa che pensa una persona con un'impostazione mentale di sicurezza è: "Posso davvero prendere un'auto semplicemente conoscendo il cognome di un cliente qualsiasi che ha la propria vettura in riparazione?"

Il resto del post riflette su come un individuo potrebbe rubare un'auto sfruttando questa vulnerabilità di sicurezza, e se abbia senso per il rivenditore essere così negligente in materia di sicurezza. Possiamo cavillare sull'analisi (sono curioso di sapere che responsabilità ha il rivenditore e se la sua assicurazione coprirebbe eventuali perdite), ma è tutta esperienza di settore. La cosa importante è anzitutto notare, e discutere, la questione sicurezza.

La mancanza di un abito mentale improntato alla sicurezza spiega molta della pessima sicurezza che vediamo dappertutto: macchine per il voto elettronico, tessere elettroniche di pagamento, attrezzature mediche, documenti di identità, protocolli Internet. I progettisti sono talmente impegnati a far funzionare questi sistemi che non si fermano a considerare come potrebbero guastarsi, o come si potrebbe indurli a fallire e come si potrebbero sfruttare tali guasti o errori. Insegnare a designer e progettisti ad avere un'impostazione mentale di sicurezza sarà un consistente passo avanti nella produzione di futuri sistemi tecnologici più sicuri.

Questa parte è ovvia, ma credo che l'impostazione mentale orientata alla sicurezza possa essere vantaggiosa anche in altri modi. Se le persone imparassero a pensare al di fuori del proprio ristretto campo visivo così da avere una visione più ampia delle cose, che si tratti di tecnologia, di politica, o della loro vita quotidiana, allora avremmo consumatori più sofisticati, cittadini più scettici e persone meno ingenui.

Se un maggior numero di persone avesse un'impostazione mentale di sicurezza, i servizi che compromettono la privacy non avrebbero una quota di mercato così grande, e Facebook sarebbe tutta un'altra cosa. Non si smarrirebbero dei portatili contenenti milioni di numeri di previdenza sociale non cifrati, e tutti apprenderebbero qualche lezione di sicurezza in più in maniera meno aspra. La rete elettrica sarebbe più sicura. I furti di identità diminuirebbero. Le informazioni sanitarie sarebbero più private. Se le persone fossero dotate dell'impostazione mentale di sicurezza, non avrebbero cercato di leggere la cartella clinica di Britney Spears, perché avrebbero capito che sarebbero state prese.

Questo particolare corso universitario non ha nulla di speciale o di magico: chiunque può esercitare il proprio abito mentale orientato alla sicurezza semplicemente provando a osservare il mondo dal punto di vista di un aggressore. Se io volessi aggirare questo particolare dispositivo di sicurezza, come farei? Potrei seguire questa legge alla lettera ma aggirandone lo spirito? Se la persona che ha scritto questo annuncio, critica, articolo o documentario televisivo avesse agito senza scrupoli, che cosa avrebbe potuto ottenere? E poi: come posso proteggermi da questi attacchi?

L'impostazione mentale di sicurezza è un'abilità assai preziosa che può avvantaggiare tutti, a prescindere dall'ambito specifico di ognuno.

SmartWater

<<http://www.smartwater.com/products/securitySolutions.html>>  
<[http://www.schneier.com/blog/archives/2005/02/smart\\_water.html](http://www.schneier.com/blog/archives/2005/02/smart_water.html)>

CSE484:

<<http://www.cs.washington.edu/education/courses/484/08wi/>>  
<<http://cubist.cs.washington.edu/Security/2007/11/22/why-a-computer-security-course-blog/>> oppure <<http://tinyurl.com/3m94ag>>

CSE484 -- il blog:

<<http://cubist.cs.washington.edu/Security/>>  
<<http://cubist.cs.washington.edu/Security/category/security-reviews/>>  
<<http://cubist.cs.washington.edu/Security/2008/03/14/security-review-michaels-toyota-service-center/>> oppure <<http://tinyurl.com/456b5y>>

Le informazioni cliniche di Britney Spears:

<<http://www.msnbc.msn.com/id/23640143>>

Questo articolo è originariamente apparso su Wired.com.

<[http://www.wired.com/politics/security/commentary/securitymatters/2008/03/securitymatters\\_0320](http://www.wired.com/politics/security/commentary/securitymatters/2008/03/securitymatters_0320)> oppure <<http://tinyurl.com/2lkg5f>>

Commenti:

<<http://www.freedom-to-tinker.com/?p=1268>>  
<<http://blog.ungullible.com/2008/03/hacking-yourself-to-ungullibility-part.html>>  
oppure <<http://tinyurl.com/3fl9np>>  
<<http://www.daemonology.net/blog/2008-03-21-security-is-mathematics.html>>  
oppure <<http://tinyurl.com/34y2en>>

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

News

Fotocamera che 'vede' sotto i vestiti:

<<http://www.reuters.com/article/technologyNews/idUSL0926757420080309>>  
Se è tutto vero, sembra una tecnologia meno invasiva rispetto ai raggi X a retrodiffusione.  
<[http://www.schneier.com/blog/archives/2005/06/backscatter\\_x-r.html](http://www.schneier.com/blog/archives/2005/06/backscatter_x-r.html)>

Quattro notizie dal Montana.

1 - La difficoltà di implementare il REAL-ID in aree così remote da non avere un Ufficio della Motorizzazione permanente.

<[http://www.economist.com/research/articlesBySubject/displaystory.cfm?subjectid=7933598&story\\_id=10751175#Thursday](http://www.economist.com/research/articlesBySubject/displaystory.cfm?subjectid=7933598&story_id=10751175#Thursday)> oppure <<http://tinyurl.com/3w7cnj>>

2 - La difficoltà di implementare la sicurezza aeroportuale in aeroporti così remoti da avere in media solo due passeggeri per volo.

<[http://www.usatoday.com/news/nation/2008-03-04-airport-screenings\\_N.htm](http://www.usatoday.com/news/nation/2008-03-04-airport-screenings_N.htm)>  
oppure <<http://tinyurl.com/2m3xlv>>

3 - Questa è la migliore: Brian Schweitzer, il governatore del Montana, parla della sua opposizione al REAL ID.

<<http://www.npr.org/templates/story/story.php?storyId=87991791>>

4 - Ancora sullo stato del Montana e il REAL-ID.

<<http://blog.wired.com/27bstroke6/2008/03/montana-gov-dhs.html>>

Nuova ricerca su come il cervello valuta i rischi.

<<http://www.sciencedaily.com/releases/2008/03/080312093854.htm>>

Squadra di artificieri disinnescò una rapa. Complimenti all'autore che ha scritto la prima frase della storia: "Una rapa cruda è stata alla radice di un allarme bomba durato ore e ore in uno studio legale".

<<http://ap.google.com/article/ALeqM5q5qxveGICNPGT6iLRiEhEUbZcepAD8VDF0A00>>

oppure <<http://tinyurl.com/37km5m>>

<<http://www.journalgazette.net/apps/pbcs.dll/article?AID=/20080315/LOCAL07/803150407/1002/LOCAL>> oppure <<http://tinyurl.com/2jug84>>

Un commento sul mio blog da parte di uno che si qualifica come l'autore dell'allarme bomba, ossia colui che ha inviato la rapa:

<[http://www.schneier.com/blog/archives/2008/03/bomb\\_squad\\_defu.html#c256420](http://www.schneier.com/blog/archives/2008/03/bomb_squad_defu.html#c256420)>

oppure <<http://tinyurl.com/4z7nko>>

Un altro dispaccio frutto della continua discesa verso lo psico-reato: una proposta da parte del Regno Unito di inserire in un database del DNA quei bambini delle scuole primarie che "esibiscono un comportamento che indichi che possano diventare criminali in età adulta". Fortunatamente l'articolo contiene alcune reazioni ragionevoli a questa proposta.

<<http://www.guardian.co.uk/society/2008/mar/16/youthjustice.children>>

Un'altra serie eccellente di post sul threat modeling (creazione di modelli di minaccia) in Microsoft, stavolta a cura di Adam Shostack.

Il primo post:

<<http://blogs.msdn.com/sdl/archive/2007/09/26/the-trouble-with-threat-modeling-2.aspx>> oppure <<http://tinyurl.com/2tvxhx>>

L'intera serie in un documento Word:

<<http://blogs.msdn.com/sdl/attachment/7702305.ashx>>

Ho già segnalato la serie scritta da Larry Osterman.

<[http://www.schneier.com/blog/archives/2007/10/threat\\_modeling.html](http://www.schneier.com/blog/archives/2007/10/threat_modeling.html)>

Malgrado la presenza di "sensori di battito cardiaco, sonde CO2 per il rilevamento di fiato espirato e scanner a 'onde millimetriche' che possono 'vedere' attraverso i veicoli", è piuttosto facile entrare di nascosto nel Regno Unito passando da Calais, grazie a barriere di recinzione inadeguate. Ricordate: la sicurezza è forte solo quanto l'anello più debole.

<[http://news.bbc.co.uk/1/hi/uk\\_politics/7277771.stm](http://news.bbc.co.uk/1/hi/uk_politics/7277771.stm)>

Idea eccentrica del mese in tema di sicurezza aerea: obbligare tutti a indossare un braccialetto che, una volta attivato a distanza, provoca uno shock debilitante alla persona. No, sul serio. Un'azienda sta cercando di mettere in commercio questa idea. C'è da inorridire al solo pensiero.

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

<<http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=%2Fnethtml%2FPTO%2Fsrchnu m.htm&r=1&f=G&l=50&s1=6,933,851.PN.&OS=PN/6,933,851&RS=PN/6,933,851>>

oppure <<http://tinyurl.com/2j6jp8>>

Questo genere di frode di carta di credito non è affatto nuovo, ma è raro trovare statistiche delle frodi vere e proprie.

<[http://www.schneier.com/blog/archives/2008/03/fraud\\_due\\_to\\_a.html](http://www.schneier.com/blog/archives/2008/03/fraud_due_to_a.html)>

Secondo me è un lavoro dall'interno.

Il rap di MC Frontalot parla di criptazione:

<<http://www.frontalot.com/index.php?page=mp3>>

<<http://www.frontalot.com/index.php?page=lyrics&lyricid=41>>

Un post davvero interessante sul potenziale futuro del calcolo quantico e dei suoi effetti sulla crittografia.

<[http://www.emergentchaos.com/archives/2008/03/quantum\\_progress.html](http://www.emergentchaos.com/archives/2008/03/quantum_progress.html)>

Risponde uno scienziato esperto in calcolo quantico:

<[http://scienceblogs.com/pontiff/2008/03/shor\\_calculations.php](http://scienceblogs.com/pontiff/2008/03/shor_calculations.php)>

Se siete pavid, credete di essere più esposti ai rischi rispetto a quando siete arrabbiati:

<<http://www.hks.harvard.edu/news-events/publications/insight/management/jennifer-lerner>> oppure <<http://tinyurl.com/3qfids>>

<[http://content.ksg.harvard.edu/lernerlab/pdfs/Lerner\\_2003\\_PS\\_Paper.pdf](http://content.ksg.harvard.edu/lernerlab/pdfs/Lerner_2003_PS_Paper.pdf)>

Costruitevi la vostra macchina Enigma di carta:

<<http://mckoss.com/Crypto/Enigma.htm>>

Una macchina Enigma sulla vecchia console Atari 2600:

<<http://brainwagon.org/the-enigma-2600/>>

Un articolo ottimo e ben scritto sulla macchina Enigma da parte della NSA:

<<http://www.nsa.gov/publications/publi00016.cfm>>

Alla DISI conference, lo scorso dicembre, Martin Hellman ha tenuto una lezione sull'invenzione della crittografia a chiave pubblica.

<<http://video.google.com/videoplay?docid=8991737124862867507>>

Questo articolo del Wall Street Journal delinea come la NSA stia occupandosi sempre più di sorveglianza nazionale, raccolta di dati e data mining. Il risultato è sostanzialmente identico al programma Total Information Awareness.

<<http://online.wsj.com/article/SB120511973377523845.html>>

I commenti di Barry Steinhardt dell'ACLU.

<<http://www.dailykos.com/storyonly/2008/3/11/14380/5939/606/474351>>

Altri commenti:

<<http://blogs.zdnet.com/Ratcliffe/?p=334&tag=nl.e622>>

Ladro ipnotizzatore in Italia. Davvero bizzarro:

<<http://news.bbc.co.uk/1/hi/world/europe/7309947.stm>>

<[http://dilbertblog.typepad.com/the\\_dilbert\\_blog/2008/03/hypnotist-thief.html](http://dilbertblog.typepad.com/the_dilbert_blog/2008/03/hypnotist-thief.html)>

oppure <<http://tinyurl.com/33xjou>>

Gli Stati Uniti hanno un nuovo 'zar' della sicurezza cibernetica, Rod A. Beckstrom, il quale non ha nessuna esperienza in materia di sicurezza cibernetica.

<<http://www.washingtonpost.com/wp-dyn/content/article/2008/03/19/AR2008031903125.html>>

oppure <<http://tinyurl.com/2yh2qv>>

<<http://arstechnica.com/news.ars/post/20080328-meet-the-new-us-cybersecurity-czar.html>> oppure <<http://tinyurl.com/2h53u6>>

Malware mirato ai danni di gruppi pro-Tibet. Pare che sia ad opera del governo cinese anche se, ovviamente, non vi è modo di provarlo.

<<http://www.f-secure.com/weblog/archives/00001406.html>>

Il post sul mio blog:

<[http://www.schneier.com/blog/archives/2008/03/malware\\_targete.html](http://www.schneier.com/blog/archives/2008/03/malware_targete.html)>

Scrittori di fantascienza offrono consigli di sicurezza nazionale. Imbarazzante.

<<http://www.nationaldefensemagazine.org/issues/2008/March/SecurityBeat.htm#Science>> oppure <<http://tinyurl.com/3a3b2z>>

Ottimo elenco delle insidie più comuni in fatto di sicurezza aziendale:

<[http://www.infoworld.com/article/08/03/17/12NF-security-landmines\\_1.html](http://www.infoworld.com/article/08/03/17/12NF-security-landmines_1.html)>

oppure <<http://tinyurl.com/2sv49l>>

L'N-DEx National Intelligence System: ulteriore raccolta di informazioni sui cittadini.

<[http://www.washingtonpost.com/wp-dyn/content/article/2008/03/05/AR2008030503656\\_pf.html](http://www.washingtonpost.com/wp-dyn/content/article/2008/03/05/AR2008030503656_pf.html)>

oppure <<http://tinyurl.com/yqoy3w>>

Il pastore di una chiesa è un ladro di identità.

<<http://www.pennlive.com/news/patriotnews/index.ssf?/base/news/120641100692450.xml&coll=1>> oppure <<http://tinyurl.com/536d4y>>

Più un ladro è una persona fidata, più sarà difficile scoprirlo.

Avete qualche idea su come produrre uno scanner di bottiglie di liquidi? La TSA ha un'offerta per voi.

<<http://www.gsnmagazine.com/cms/resources/business-opportunities/624.html>>

oppure <<http://tinyurl.com/2bo5c9>>

Quantum Sleeper Unit: creazione di spauracchi e messinscena di sicurezza come non mai.

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

Il Chaos Computer Club ha pubblicato l'impronta digitale del ministro degli interni tedesco Wolfgang Schauble. Si tratta di 1) un'ottima dimostrazione del fatto che un'impronta non è segreta e 2) un'operazione di hacking politico eccellente. Schauble è un gran sostenitore della raccolta di dati biometrici di tutti come misura antiterrorismo. Perché... beh, perché sembra una buona idea.

<[http://www.theregister.co.uk/2008/03/30/german\\_interior\\_minister\\_fingerprint\\_appropriated/](http://www.theregister.co.uk/2008/03/30/german_interior_minister_fingerprint_appropriated/)> oppure <<http://tinyurl.com/2husjv>>

<<http://www.heise.de/english/newsticker/news/105728>>

<<http://www.ccc.de/updates/2008/schaubles-finger>>

L'impronta stessa, pronta da stampare:

<<http://www.ccc.de/images/misc/schaeuble-attrappe.png>>

Guida in inglese su come raccogliere e utilizzare le impronte digitali.

<[http://www.ccc.de/biometrie/fingerabdruck\\_kopieren?language=en](http://www.ccc.de/biometrie/fingerabdruck_kopieren?language=en)>

Il mio articolo di dieci anni fa sui dati biometrici:

<<http://www.schneier.com/crypto-gram-9808.html#biometrics>>

Gli Stati Uniti stanno esternalizzando la costruzione dei passaporti RFID ad aziende di dubbia reputazione. Ciò illustra ottimamente la massima "I compromessi di sicurezza

vengono spesso creati per ragioni non legate alla sicurezza". Già mi immagino il manager in carica: "Sì, non è sicuro. Ma pensate a quanto si risparmia!"

<<http://washingtontimes.com/apps/pbcs.dll/article?AID=/20080326/NATION/%20840186493/0/BUSINESS>> oppure <<http://tinyurl.com/345f6u>>

<[http://www.upi.com/NewsTrack/Top\\_News/2008/03/26/outsourcing\\_passports\\_profo\\_und\\_liability/9799/](http://www.upi.com/NewsTrack/Top_News/2008/03/26/outsourcing_passports_profo_und_liability/9799/)> oppure <<http://tinyurl.com/26u35h>>

L'Australia potrebbe mettere fuori legge i puntatori laser perché sono stati utilizzati contro degli aerei lo scorso mese. Sono certo che i criminali hanno anche usato delle automobili la scorsa settimana. Saranno le prossime a essere vietate? D'altro canto io stesso sono stufo marcio dei puntatori laser. Ma i gatti australiani saranno tremendamente delusi.

<<http://www.smh.com.au/news/national/lasers-face-import-ban/2008/03/30/1206850709183.html>> oppure <<http://tinyurl.com/4v3kzk>>

Un articolo dell'Atlantic del 1967 che dimostra una paurosa preveggenza sul futuro della privacy delle informazioni e della sicurezza. Presenta tutte le argomentazioni base per controlli più severi sulla raccolta di informazioni personali, ed è straordinariamente accurato nelle sue predizioni sul futuro sviluppo e importanza dei computer, e sui vari modi utilizzati dal governo per abusarne. Una lettura obbligatoria.

<<http://blog.modernmechanix.com/2008/03/31/the-national-data-center-and-personal-privacy/>> oppure <<http://tinyurl.com/2rg864>>

Il Defendius Labyrinth Security Lock è un pesce d'aprile, ma ne voglio uno lo stesso.

<<http://www.thinkgeek.com/stuff/41/titaniumlabyrinth.html?cpg=70H>>

Abbiamo finalmente qualche informazione vera sulla 'bomba liquida' che quel gruppo arrestato a Londra nel 2006 aveva intenzione di utilizzare: "La corte ha sentito che i dinamitardi erano intenzionati a impiegare perossido di idrogeno mischiato con un prodotto chiamato Tang, utilizzato in bevande analcoliche, per trasformarlo in esplosivo. Volevano portarlo a bordo camuffato da bottiglie da 50 cl di Oasis o Lucozade utilizzando coloranti alimentari per ricreare i colori tipici delle bevande. Il detonatore sarebbe stato camuffato sotto forma di pile stilo AA da 1,5 V; il contenuto delle pile sarebbe stato eliminato per inserire un elemento elettrico, come una lampadina o del filo di rame. Una macchina fotografica usa-e-getta avrebbe fornito l'energia necessaria".

<[http://www.dailymail.co.uk/pages/live/articles/news/news.html?in\\_article\\_id=555465&in\\_page\\_id=1770&ct=5](http://www.dailymail.co.uk/pages/live/articles/news/news.html?in_article_id=555465&in_page_id=1770&ct=5)> oppure <<http://tinyurl.com/2xnabh>>

Molti i commenti sul mio blog in merito alla fattibilità di tutto questo:

<[http://www.schneier.com/blog/archives/2008/04/the\\_liquid\\_bomb.html](http://www.schneier.com/blog/archives/2008/04/the_liquid_bomb.html)>

Il sistema di ingresso 'senza chiave' KeeLoq viene impiegato da Chrysler, Daewoo, Fiat, General Motors, Honda, Toyota, Lexus, Volvo, Volkswagen, Jaguar e probabilmente da altre marche. È stato craccato.

<<http://www.crypto.rub.de/keeloq/index.html>>

<[http://www.theregister.co.uk/2008/04/03/keeloq\\_master\\_key\\_found/](http://www.theregister.co.uk/2008/04/03/keeloq_master_key_found/)>

Una vicenda bizzarra. Uno scassinatore si crea una copertura pubblicando un finto annuncio su Craigslist dicendo che il proprietario di una casa ha dovuto partire all'improvviso e che tutti i suoi averi erano liberamente disponibili. Poi va a rubare, così come tutti quelli che hanno preso l'annuncio per vero.

<[http://www.schneier.com/blog/archives/2008/03/craigslist\\_scam.html](http://www.schneier.com/blog/archives/2008/03/craigslist_scam.html)>

Un potenziale dinamitardo è stato catturato all'Orlando Airport grazie al profiling comportamentale. Qui i miei commenti:

<[http://www.schneier.com/blog/archives/2008/04/wouldbe\\_bomber\\_1.html](http://www.schneier.com/blog/archives/2008/04/wouldbe_bomber_1.html)>

Dati provenienti da San Francisco che dimostrano l'inefficacia delle telecamere di sicurezza. Questo passaggio è istruttivo: "Il sindaco Gavin Newsom ha definito il rapporto 'definitivamente inconcludente' lo scorso giovedì, ma ha dichiarato che vuole comunque installare più telecamere in città perché fanno sentire i residenti più sicuri". Ma certo: le telecamere non hanno niente a che fare con la sicurezza, ma con la messinscena di sicurezza. Ulteriori commenti sulla problematica in generale:

<<http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2008/03/21/MN27VNFET.DTL>>

oppure <<http://tinyurl.com/2h4d65>>

<<http://gritsforbreakfast.blogspot.com/2005/03/why-surveillance-cameras-dont-reduce.html>> oppure <<http://tinyurl.com/4r9qt>>

<<http://gritsforbreakfast.blogspot.com/2008/04/best-way-to-terminate-surveillance.html>> oppure <<http://tinyurl.com/3oqzz7>>

La NSA ha rilasciato la propria versione di Linux. E dunque, vi fidate?

<[http://www.upi.com/International\\_Security/Emerging\\_Threats/Briefing/2008/03/24/nsa\\_releases\\_new\\_version\\_of\\_linux\\_software/9918/](http://www.upi.com/International_Security/Emerging_Threats/Briefing/2008/03/24/nsa_releases_new_version_of_linux_software/9918/)>

oppure <<http://tinyurl.com/6bzc2f>>

La guida della NSA per rendere Linux sicuro:

<<http://www.nsa.gov/snac/os/redhat/rhel5-guide-i731.pdf>>

Sempre più college offrono titoli in sicurezza nazionale:

<<http://www.slate.com/?id=2187648>>

Tenere sotto controllo i veicoli attraverso dispositivi che monitorano la pressione degli pneumatici: uno dei tanti esempi della sorveglianza prossima ventura.

<<http://www.hexview.com/sdp/node/44>>

<<http://www.canadiandriver.com/articles/jk/070404.htm>>

<<http://www.canadiandriver.com/articles/jm/tpms2.htm>>

Ottimo articolo di una madre che ha lasciato che il proprio figlio di 9 anni andasse da solo sulla metropolitana di New York, e tutta la discussione è indicativa di quanto sopravvalutiamo le minacce contro i bambini:

<<http://www.schneier.com/blog/archives/2008/04/overestimating.html>>

Esiste un progetto per creare un sistema d'allarme a livello nazionale che faccia uso dei messaggi SMS. Quel che bisogna davvero chiedersi è se i benefici siano maggiori dei rischi. Posso sicuramente immaginare delle situazioni in cui l'invio di brevi messaggi di testo alla popolazione di una certa area geografica sia un'ottima idea, ma posso anche immaginare le varie possibilità offerte dall'hacking di tale sistema. E una volta che questo sistema verrà sviluppato per le emergenze, si farà certamente strada un business dei messaggi SMS all'ingrosso.

<[http://www.schneier.com/blog/archives/2008/04/bulk\\_text\\_messa.html](http://www.schneier.com/blog/archives/2008/04/bulk_text_messa.html)>

In questo articolo che analizza una falla di sicurezza che ha provocato l'invio in aria di testate nucleari sopra gli Stati Uniti, vi è un commento interessante sulle persone e sulle procedure di sicurezza: "Non dimentichiamo che le procedure in atto erano davvero rigorose", ha dichiarato Hans Kristensen, direttore del Nuclear Information

Project for the Federation of American Scientists. 'Molto di quel che è andato storto è accaduto perché la gente non ha seguito quelle regole severe. Potete stabilire tutte le norme e regolamentazioni che volete, ma non serviranno a nulla se la gente non le osserva'".

È difficile raggiungere un equilibrio con le procedure. Se sono troppo permissive, vi saranno problemi di sicurezza. Se sono troppo rigorose, la gente le eluderà e vi saranno problemi di sicurezza.

<<http://www.military.com/features/0,15240,165396,00.html>>

Il Pentagono potrebbe fornire delle macchine della verità tascabili ai soldati americani in Afghanistan, anche se non funzionano come dovrebbero.

<<http://www.msnbc.msn.com/id/23926278/>>

Un buon articolo sulla difficoltà di tenere le droghe fuori dai penitenziari. Esistono molti modi per aggirare la sicurezza, fra cui il servirsi di guardiani corrotti.

<<http://news.bbc.co.uk/go/em/fr/-/1/hi/magazine/7340533.stm>>

Ho già scritto in merito al RIPA (Regulation of Investigatory Powers Act) del Regno Unito, che è stato pubblicizzato come un mezzo per combattere il terrorismo e altri gravi crimini, quando poi è stato usato contro i sostenitori dei diritti degli animali. Le ultime nuove dal Regno Unito: un consiglio locale si è servito di alcuni provvedimenti di tale legge per mettere sotto sorveglianza una coppia di persone e i loro figli, per "sospette attività fraudolente in luoghi scolastici". Questo genere di cose continua a succedere. Quando sostengono l'approvazione di una legge, le autorità invocano i peggiori criminali: terroristi, sequestratori, spacciatori di droga, pedopornografi. Ma una volta che la legge viene approvata, iniziano a usarla in situazioni molto più banali.

<<http://news.bbc.co.uk/1/hi/england/dorset/7341179.stm>>

<[http://www.theregister.co.uk/2008/04/11/poole\\_council\\_ripa/](http://www.theregister.co.uk/2008/04/11/poole_council_ripa/)>

<[http://www.schneier.com/blog/archives/2007/11/animal\\_rights\\_a.html](http://www.schneier.com/blog/archives/2007/11/animal_rights_a.html)>

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

## Percezione e realtà della sicurezza

La sicurezza è sia una percezione che una realtà, e sono due cose assai diverse. Potreste sentirvi sicuri pur non essendolo davvero, e potreste essere realmente al sicuro pur non avendone l'impressione. Vi sono due distinti concetti associati alla stessa parola (la lingua inglese non ci aiuta molto in questo contesto) e può essere difficile capire di quale stiamo parlando quando utilizziamo la parola sicurezza.

È estremamente importante separare i due concetti, spiegarne le differenze e comprendere quando ci si riferisce all'uno o all'altro. Ed è altrettanto importante riconoscere quando i due concetti convergono, capire perché divergono, e sapere come è possibile farli convergere nuovamente.

Prima alcune premesse basilari. Dal punto di vista economico, la sicurezza è un compromesso. Non esiste la sicurezza assoluta, e qualsiasi sicurezza si ottenga avrà sempre un costo: in denaro, in comodità, in possibilità, in insicurezze da qualche altra parte, e così via. Ogni volta che qualcuno effettua una decisione di sicurezza (sicurezza informatica, sicurezza della comunità, sicurezza nazionale), crea un compromesso.

La gente crea simili compromessi a livello individuale. Tutti decidiamo individualmente se la spesa e l'impiccio di avere un allarme antifurto in casa vale la sicurezza che offre. Tutti noi decidiamo se indossare un giubbotto antiproiettile ne vale il costo e l'apparire un po' ridicoli. Tutti noi decidiamo se i miliardi di dollari spesi nella lotta al terrorismo siano soldi ben investiti, e se l'invasione dell'Iraq sia stato il modo migliore di impiegare le nostre risorse antiterrorismo. Magari non abbiamo il potere di "implementare" la nostra opinione, ma comunque arriviamo a decidere se, in cuor nostro, crediamo ne valga la pena.

Potremmo avere o non avere l'esperienza necessaria a creare quei compromessi in maniera intelligente, ma li facciamo ugualmente. Tutti noi. Le persone hanno un'intuizione naturale per quanto riguarda i compromessi di sicurezza, e li facciamo, grandi e piccoli, decine di volte in una giornata. Non possiamo farne a meno: è parte del nostro vivere.

Immaginiamo un coniglio che brucia l'erba in un prato. Vede una volpe. A quel punto stabilirà un compromesso di sicurezza: rimanere o fuggire via? Col tempo, i conigli che si dimostrano capaci di effettuare quel compromesso tenderanno a riprodursi, mentre i conigli che non ne sono capaci avranno la tendenza a essere divorati o a morire di fame.

Per cui, considerando il successo della specie umana sul pianeta, ci si aspetterebbe dagli esseri umani un'ottima capacità di effettuare compromessi di sicurezza. Però, allo stesso tempo, riusciamo a fare enormi pasticci in questo campo. Spendiamo più denaro nella lotta al terrorismo di quanto ci indichino le informazioni a riguardo. Abbiamo paura di volare e scegliamo di guidare un'automobile. Perché?

La risposta breve è che le persone effettuano la maggior parte dei compromessi di sicurezza basandosi sulla "percezione" della sicurezza e non sulla "realtà".

Ho scritto molto su come la gente sbaglia nell'affrontare i compromessi di sicurezza, e sui bias cognitivi che ci fanno commettere errori. Gli esseri umani hanno sviluppato tali bias perché hanno senso da un punto di vista evolutivo. E nella maggior parte dei casi funzionano.

Nella maggior parte dei casi, e questo è importante, la nostra percezione di sicurezza coincide con la realtà della sicurezza. Di sicuro vale per la preistoria. I tempi moderni sono più difficili. Possiamo dare la colpa alla tecnologia, ai media, a qualunque cosa. Il nostro cervello è molto più ottimizzato per i compromessi di sicurezza legati alla vita in piccoli gruppi familiari nelle zone montagnose dell'Africa Orientale del 100.000 a.C. che non a quelli legati alla vita nella città di New York nel 2008.

Se creiamo compromessi di sicurezza basati sulla percezione di sicurezza invece che sulla realtà della sicurezza, scegliamo una sicurezza che ci fa "sentire" più al sicuro rispetto a una sicurezza che ci protegge davvero. Ed è quanto offrono i governi, le aziende, i membri di una famiglia e tutti gli altri. Ovviamente vi sono due modi di far sentire la gente più al sicuro. Il primo è di proteggerla veramente e sperare che se ne accorga. Il secondo è di far sentire le persone più al sicuro ma senza proteggerle realmente, e sperare che non se ne accorgano.

Il punto essenziale qui è accorgersene o no. La percezione e la realtà della sicurezza tendono a convergere quando ce ne accorgiamo, e a divergere quando non ce ne accorgiamo. Le persone se ne accorgono quando 1) esiste un numero sufficiente di esempi positivi e negativi per tirare una conclusione, e 2) la questione non è offuscata da un eccesso di emotività.

Entrambi questi elementi sono importanti. Se qualcuno cerca di convincerci a spendere soldi per un nuovo tipo di allarme antifurto, noi in quanto società sapremo molto presto se questa persona ha sviluppato un dispositivo di sicurezza davvero innovativo o se è soltanto un ciarlatano: possiamo controllare i tassi di criminalità. Ma se quella stessa persona sostiene un nuovo sistema antiterrorismo nazionale, e non ci sono stati attacchi terroristici né prima né dopo l'implementazione di tale sistema, come facciamo a stabilirne l'efficacia?

Le persone tendono più spesso a valutare realisticamente tali incidenti se non contraddicono dei preconcetti su come funziona il mondo. Per esempio: è ovvio che un muro serve a tenere la gente alla larga, per cui è più difficile opporsi alla costruzione di un muro lungo il confine meridionale degli Stati Uniti per evitare l'ingresso di immigranti clandestini.

Un altro fattore importante è l'agenda. Vi sono molte persone, uomini politici, industrie, ecc., che provano deliberatamente a manipolare la nostra percezione di sicurezza a loro vantaggio. Cercano di provocare paura. Si inventano le minacce. Prendono minacce di poca importanza e le ingigantiscono. E quando si mettono a parlare di rischi rari valutabili soltanto in base a pochissimi incidenti (come nel caso del terrorismo), hanno maggiori probabilità di successo.

Sfortunatamente non esiste un facile antidoto. L'informazione è importante. Non possiamo capire come funziona la sicurezza se non la comprendiamo. Ma non basta: pochi fra noi comprendono veramente il cancro, tuttavia prendiamo continuamente decisioni di sicurezza calcolandone il rischio. Quel che facciamo è accettare che esistano esperti che comprendono i rischi del cancro, e lasciamo che siano loro a effettuare i compromessi di sicurezza per noi.

Vi sono dei cicli complessi di feedback in azione, fra emozione e ragione, fra la realtà e la nostra conoscenza di essa, fra percezione e familiarità, e fra il comprendere come ragioniamo e come ci sentiamo in relazione alla sicurezza e le nostre analisi e sentimenti. Non smetteremo mai di effettuare compromessi di sicurezza basati sulla nostra percezione di sicurezza, e non riusciremo mai a impedire del tutto a chi ha degli interessi specifici di volersi prendere cura di noi. Ma più ne sappiamo, migliori saranno i compromessi che stabiliremo.

Gli errori nei compromessi di sicurezza:

<<http://www.schneier.com/essay-162.html>>

Bias cognitivi che influiscono sulla sicurezza:

<<http://www.schneier.com/essay-155.html>>

"Elogio alla messinscena di sicurezza":

<<http://www.schneier.com/essay-154.html>>

Il mercato dei 'bidoni' di sicurezza:

<<http://www.schneier.com/essay-165.html>>

Sicurezza aerea e agenda:

<[http://www.schneier.com/blog/archives/2005/08/airline\\_security\\_2.html](http://www.schneier.com/blog/archives/2005/08/airline_security_2.html)>

Questo articolo è originariamente apparso su Wired.com.

<[http://www.wired.com/politics/security/commentary/securitymatters/2008/04/securitymatters\\_0403](http://www.wired.com/politics/security/commentary/securitymatters/2008/04/securitymatters_0403)> oppure <<http://tinyurl.com/2xu2zb>>

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

## Intrappolamento Web

Spaventosa operazione di polizia dell'FBI. Ha pubblicato link a presunti video pedopornografici in forum frequentati da pedofili, e ha ottenuto mandati di perquisizione basandosi sui tentativi di accesso a quei link.

Sembrano prove incredibilmente deboli e inconsistenti. Uno potrebbe pubblicare il link come immagine incorporata, o inviare email con il link incorporato, e alterare totalmente i dati dell'FBI (e causare danni alle vite di poveri innocenti). Questi sono i problemi quando il semplice clic su un link diventa un pretesto per un mandato.

<[http://www.news.com/8301-13578\\_3-9899151-38.html?tag=nefd.pop](http://www.news.com/8301-13578_3-9899151-38.html?tag=nefd.pop)>

<<http://yro.slashdot.org/yro/08/03/20/2323247.shtml>>

<<http://arstechnica.com/news.ars/post/20080323-rick-rolled-to-child-porn-youre-a-pedophile-says-fbi.html>> oppure <<http://tinyurl.com/2ffhs2>>

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

## Le news su Schneier/BT Counterpane

Interviste a Schneier:

<<http://www.scienceprogress.org/2008/03/the-halfway-house-between-science-and-secrets/>> oppure <<http://tinyurl.com/2f483v>>

<[http://www.ebizq.net/blogs/news\\_security/2008/03/does\\_the\\_security\\_industry\\_hav.php](http://www.ebizq.net/blogs/news_security/2008/03/does_the_security_industry_hav.php)> oppure <<http://tinyurl.com/27udzp>>

<[http://flashplayer.streamos.com/flvplayer.php?url=http://rsa.edgeboss.net/flash/rsa/rsaconference/2008/us/podcasts/bruce\\_schneier.mp3](http://flashplayer.streamos.com/flvplayer.php?url=http://rsa.edgeboss.net/flash/rsa/rsaconference/2008/us/podcasts/bruce_schneier.mp3)>

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

<[http://rsa.edgeboss.net/download/rsa/rsaconference/2008/us/podcasts/bruce\\_schneier.mp3](http://rsa.edgeboss.net/download/rsa/rsaconference/2008/us/podcasts/bruce_schneier.mp3)> oppure <<http://tinyurl.com/4vqssb>>

<<http://www.schneier.com/news-055.html>>

Schneier intervorrà alla Hack-in-the-Box Security Conference a Dubai il 16 aprile:

<<http://conference.hitb.org/hitbsecconf2008dubai/>>

Schneier intervorrà alla IT Security and Society Conference a Eindhoven, Olanda, il 21 aprile:

<<http://www.win.tue.nl/eipsi/>>

Schneier interverrà a InfoSecurity Europe a Londra il 23 aprile:

<<http://www.infosec.co.uk/>>

Schneier parlerà all'Universitat Autònoma de Barcelona a Barcellona, Spagna, il 24 aprile:

<[http://www.uab.es/anycomputacio/cicles\\_activitats2.htm](http://www.uab.es/anycomputacio/cicles_activitats2.htm)>

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

### Autovelox e conflitti di interessi

Se vi serve un esempio per dimostrare che la sicurezza è in funzione dell'agenda e di interessi specifici, prendete questa storia sugli autovelox. Le città che hanno installato gli autovelox scoprono che gli automobilisti stanno guidando più lentamente e con prudenza, il che fa diminuire i ricavi prodotti dalle multe. Allora disattivano gli autovelox.

Le multe non dovrebbero mai essere considerate parte di un flusso di entrate: questo offre alla polizia un incentivo tutto nuovo, un incentivo che è meglio non abbia.

<<http://www.msnbc.msn.com/id/23710970>>

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

### Cinture di sicurezza e comportamento compensativo

Esiste una teoria secondo la quale le persone possiedono una sorta di termostato interno del rischio che cerca continuamente un livello ottimale di rischio. Quando qualcosa diventa intrinsecamente più sicuro, per esempio viene approvata una legge che obbliga i motociclisti a indossare un casco, le persone compensano conducendo in maniera più imprudente. Mi sono imbattuto per la prima volta in questa teoria nel 1999 leggendo uno studio di John Adams dell'Università di Reading, anche se pare sia stata originata da Sam Peltzman.

In ogni caso, un nuovo studio presenta dei dati che contraddicono quella tesi: "Questo studio analizza gli effetti che le leggi sull'obbligo delle cinture di sicurezza hanno sul comportamento degli automobilisti e sulle morti per incidenti stradali. Servendoci di un unico set di dati sull'utilizzo delle cinture di sicurezza in tutte le giurisdizioni statunitensi, analizziamo come tali leggi sull'impiego delle cinture di sicurezza influiscano sull'incidenza delle morti dovute a incidenti stradali. Tenendo conto della endogeneità dell'uso delle cinture di sicurezza, abbiamo notato che tale uso fa diminuire in generale il numero di morti dovute a incidenti stradali. L'importanza di questo effetto, tuttavia, è considerevolmente minore delle stime della National Highway Traffic Safety Administration. Inoltre non abbiamo trovato un supporto significativo alla teoria del comportamento compensativo, secondo cui l'uso delle cinture di sicurezza avrebbe anche un effetto indiretto e avverso sul numero di morti spingendo a una

guida meno prudente. Infine abbiamo identificato alcuni fattori, specialmente il tipo di legge utilizzato, che rendono più efficaci le leggi sull'obbligo delle cinture di sicurezza".

<<http://www.stanford.edu/~leinav/pubs/RESTAT2003.pdf>>

John Adams:

<<http://www.cato.org/pubs/pas/pa-335es.html>>

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

Internet e la censura

Una recensione di "Access Denied", a cura di Ronald Deibert, John Palfrey, Rafal Rohozinski e Jonathan Zittrain, MIT Press: 2008.

Nel 1993, il pioniere di Internet John Gilmore disse: "La rete interpreta la censura come un danno, e continua a funzionare aggirandola", e gli abbiamo creduto. Nel 1996, il fautore delle cyber-libertà John Perry Barlow pubblicò la sua 'Dichiarazione di Indipendenza del Cyberspazio' al World Economic Forum a Davos, in Svizzera, e anche online. Egli disse ai governi: "Non avete alcun diritto morale di dominarci, né siete in possesso di alcuno strumento di potere che ci faccia davvero paura".

A quei tempi, molti condividevano la posizione di Barlow. Internet dava potere alle persone. Offriva loro accesso alle informazioni e non poteva essere fermata, bloccata o filtrata. Date a una persona la possibilità di accedere a Internet, e questi avrà accesso a tutto. I governi che si affidavano alla censura per controllare i propri cittadini erano minacciati.

Oggi le cose sono molto diverse. La censura in Internet sta prosperando. Le organizzazioni bloccano l'accesso a Internet dei propri dipendenti in maniera selettiva. Almeno 26 paesi (specie nel Medio Oriente, nel Nord Africa, in Asia, nel Pacifico e nell'ex Unione Sovietica) bloccano in modo selettivo l'accesso a Internet ai propri cittadini. E sempre più paesi emanano leggi per controllare quel che può e non può essere detto, scaricato o referenziato. "Non avete sovranità sui luoghi in cui ci riuniamo", aveva detto Barlow. Oh sì che l'abbiamo, hanno risposto i governi di tutto il mondo.

"Access Denied" è un sondaggio sulla pratica del filtraggio di Internet, e una raccolta di dettagli sui paesi che lo effettuano. È scritto da ricercatori dell'OpenNet Initiative (ONI), un'organizzazione dedicata a documentare il filtraggio Internet che avviene in tutto il mondo.

La prima metà del libro raccoglie studi scritti dai ricercatori dell'ONI sulla politica, sulla pratica, sulla tecnologia, sulla legalità e sugli effetti sociali del filtraggio di Internet. Vi sono tre ragioni fondamentali alla base della censura in Internet: politica e potere; costumi, moralità e religione; problematiche di sicurezza.

Alcuni paesi, come l'India, filtrano solo alcuni siti; altri, come l'Iran, filtrano Internet più estesamente. L'Arabia Saudita cerca di bloccare tutta la pornografia (costumi e moralità). La Siria blocca tutto quel che proviene dal dominio ".il" di Israele (politica e

potere). Altri paesi filtrano solo in alcune occasioni. Durante le elezioni del 2006 in Bielorussia, per esempio, il sito Web del principale candidato dell'opposizione scomparve da Internet.

L'efficacia del filtraggio di Internet è variabile; dipende dagli strumenti impiegati e dalla granularità del filtraggio. È molto più facile bloccare certi URL o interi domini che non impedire la circolazione di informazioni su un determinato argomento. Alcuni paesi bloccano siti o URL specifici basandosi su degli elenchi predefiniti, ma nuovi URL dai contenuti simili continuano a saltar fuori. Altri paesi (la Cina in primis) cercano di filtrare sulla base di parole chiave contenute nelle stesse pagine Web. Una contromisura mediamente efficace è quella di filtrare sulla base di parole chiave negli URL: nomi di dissidenti o di partiti politici, oppure parole legate al sesso.

Gran parte della tecnologia impiegata ha anche altre applicazioni. Il software per il filtraggio è una categoria di prodotti più che legittima, acquistata dalle scuole per evitare che i bambini abbiano accesso a contenuti discutibili, e dalle aziende per evitare che i dipendenti si distraggano durante il lavoro. Un capitolo tratta le implicazioni etiche di certe compagnie che vendono prodotti, servizi e tecnologie che permettono la censura in Internet.

Certa censura è legale e non tecnica. Vi sono dei paesi che hanno leggi contro la pubblicazione di determinati contenuti, requisiti di registrazione per impedire l'utilizzo anonimo di Internet, leggi di responsabilità che obbligano i fornitori di accesso Internet a fungere essi stessi da filtro, oppure a sorvegliare il traffico dei propri utenti. L'Egitto non effettua un filtraggio tecnico di Internet: le sue leggi, invece, scoraggiano la pubblicazione e la lettura di certi contenuti. Alcune persone sono persino finite in prigione a causa delle loro attività online.

La seconda metà di "Access Denied" è composta da descrizioni dettagliate dell'utilizzo di Internet, delle leggi e della censura in otto regioni del mondo, e in 40 paesi diversi. L'ONI ha trovato prove che dimostrano che in 26 di quei 40 paesi è in atto una qualche forma di censura. Per i restanti 14 paesi viene riassunto lo schema legislativo riguardante l'uso di Internet, e vengono verificati i risultati che hanno indicato assenza di censura. Questo porta a 200 pagine un po' sterili, ma è di vitale importanza che queste informazioni siano ben documentate e accessibili. I dati del libro sono del 2006, ma gli autori promettono frequenti aggiornamenti sul sito Web della ONI.

Nessuna serie di misure di censura in Internet è perfetta. Spesso è facile trovare le stesse informazioni su URL non censurati, ed è abbastanza semplice aggirare i meccanismi di filtraggio e visitare pagine Web proibite se si sa quel che si sta facendo. Ma molte persone non hanno le capacità informatiche per aggirare i controlli, e in un paese in cui ciò è punibile con il carcere, o peggio, pochi hanno voglia di correre il rischio. Per cui anche quei tentativi di censura permeabile e poco efficace possono rivelarsi molto validi socialmente e politicamente.

Nel 1996 Barlow disse: "State cercando di respingere il virus della libertà costruendo torri di guardia alle frontiere del cyberspazio. Queste potranno tenere a bada il contagio per un certo tempo, ma non avranno effetto in un mondo che presto sarà dominato dai media basati sui bit".

Parole coraggiose, ma premature. Sicuramente oggi vi sono molte più informazioni accessibili da molte più persone rispetto alla realtà del 1996. Ma Internet è fatta di

computer e connessioni fisiche che esistono all'interno di confini nazionali. L'Internet di oggi continua ad avere frontiere e i vari paesi vogliono controllare sempre di più quel che passa attraverso tali frontiere. Nel documentare questo controllo, l'ONI ha fornito un servizio assai prezioso.

OpenNet Initiative:

<<http://www.opennet.net>>

Questo articolo è stato originariamente pubblicato in Nature:

<<http://www.nature.com/nature/journal/v452/n7184/full/452155b.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](mailto:crypto-gram@communicationvalley.it)>

I commenti a CRYPTO-GRAM devono essere inviati a [schneier@counterpane.com](mailto: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.