

CRYPTO-GRAM
15 febbraio 2009

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:

- Aiutare i terroristi
- Fuga di informazioni di Monster.com
- News
- La regola di esclusione delle prove e la sicurezza
- La garanzia di BitArmor contro la fuga di informazioni
- Le news su Schneier
- Le leggi sulla notifica della perdita di informazioni
- Commenti dei lettori

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

Aiutare i terroristi

Il pubblico rimane costantemente sorpreso dal fatto che la nostra infrastruttura possa venire usata contro di noi. E a seguito di attacchi o complotti terroristici emergono svariate richieste, alimentate dalla paura, di porre dei divieti, di smantellare o controllare quell'infrastruttura. Secondo le autorità che stanno investigando gli attacchi di Mumbai, i terroristi si sono serviti di immagini ottenute da Google Earth per orientarsi e pianificare le loro mosse. Questa non è la prima volta che Google Earth è stato accusato di essere uno strumento che aiuta i terroristi: nel 2007, immagini di basi militari britanniche prese da Google Earth vennero scoperte nelle case di insorgenti iracheni. Incidenti come questo hanno spinto molti governi a ordinare a Google di eliminare o sfuocare immagini di luoghi sensibili: basi militari, reattori nucleari, edifici

governativi, e così via. A un tribunale in India è stato chiesto di vietare Google Earth completamente.

Questa non è l'unica maniera in cui la nostra tecnologia dell'informazione aiuta i terroristi. Lo scorso anno, un rapporto di intelligence dell'esercito americano paventava la possibilità che i terroristi potessero pianificare i loro attacchi utilizzando Twitter, e vi sono rapporti ancora non confermati secondo cui i terroristi di Mumbai leggevano i feed di Twitter riguardanti i loro attacchi per ottenere informazioni utili in tempo reale. I servizi segreti britannici sono preoccupati che i terroristi possano ricorrere a servizi di Voice over IP, come Skype, per comunicare fra loro. I terroristi potrebbero persino reclutare nuovi membri su Second Life e World of Warcraft. Già sappiamo che si servono di siti Web per diffondere il loro messaggio e forse anche per reclutare seguaci.

Naturalmente, tutto questo è aggravato dall'accesso open-wireless, che è stato più volte definito strumento terroristico e che si è cercato più volte di vietare.

Anche le reti di telefonia mobile aiutano i terroristi. A Mumbai i terroristi le hanno utilizzate per comunicare fra loro. Ciò ha portato alcune città, fra cui New York e Londra, a proporre la disattivazione della rete cellulare in caso di attacco terroristico.

Bene, adesso fermiamoci e prendiamo un bel respiro. Per la sua propria natura, l'infrastruttura delle comunicazioni è generale. Può essere impiegata per pianificare sia attività lecite che illecite, e in linea di massima è impossibile poterle distinguere. Quando spedisco e ricevo delle email, tale processo è indistinguibile da quello di un terrorista che spedisce e riceve email. Per una rete di telefonia mobile, una chiamata fra due terroristi appare del tutto identica a una chiamata fra due vittime. Qualsiasi tentativo di vietare o limitare l'infrastruttura danneggia tutti noi. Se l'India vieta del tutto Google Earth, un futuro terrorista non potrà servirsene per i suoi piani -- né potrà essere utilizzato dal resto della gente. Le reti Wi-Fi aperte sono utili per svariate ragioni, per la maggior parte positive, e chiudere quelle reti significa eliminarne i benefici per tutti. Gli attacchi terroristici sono assai rari, ed è quasi sempre un pessimo compromesso negare alla società i vantaggi di una tecnologia per le comunicazioni soltanto perché potrebbe venire impiegata anche dai criminali.

L'infrastruttura di comunicazione è preziosa specialmente durante un attacco terroristico. Twitter è stato il sistema migliore per ottenere informazioni in tempo reale su quel che stava accadendo a Mumbai. Se il governo indiano bloccasse Twitter - o se Londra disattivasse la rete cellulare - durante un attacco terroristico, la mancanza di comunicazioni per tutti, non solo per i terroristi, aumenterebbe il livello di terrore e potrebbe persino incrementare il numero di morti. L'informazione riduce la paura e rende le persone più sicure.

Ma nulla di tutto questo è una novità. I criminali hanno utilizzato telefoni e cellulari sin da quando furono inventati. I trafficanti di droga fanno uso di aerei e imbarcazioni, di radio e telefoni satellitari. I rapinatori di banche da sempre usano automobili e motociclette per svignarsela, e prima usavano i cavalli. Non ho ancora visto una discussione a riguardo, ma i terroristi di Mumbai si sono serviti anche di imbarcazioni. Indossavano anche stivali. Hanno pranzato in ristoranti e bevuto acqua minerale e respirato l'aria. La società continua ad andare avanti perché gli usi legittimi dell'infrastruttura superano di gran lunga gli usi illeciti, malgrado i primi siano in gran parte banali e diffusi e i secondi rari e spettacolari. E mentre il terrorismo mette l'infrastruttura della società contro se stessa, noi non facciamo altro che danneggiarci

ulteriormente se rispondiamo smantellando quella stessa infrastruttura, analogamente a quanto accadrebbe se proibissimo l'uso delle automobili perché vengono utilizzate anche dai rapinatori di banche.

Google Earth aiuta i terroristi:

<<http://news.nationalgeographic.com/news/2007/03/070312-google-censor.html>>
oppure <<http://tinyurl.com/23nlat>>
<http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article5311241_ece>
oppure <<http://tinyurl.com/5htbj6>>
<http://news.cnet.com/How-law-enforcement-uses-Google-Earth/2100-1025_3-6208034.html>
oppure <<http://tinyurl.com/d6w6h2>>

Twitter aiuta i terroristi:

<<http://www.inquisitr.com/9863/report-indian-government-trying-to-block-twitter-as-terrorists-may-be-reading-it/>>
oppure <<http://tinyurl.com/566bt2>>
<<http://bit.ly/terror4>>

Skype aiuta i terroristi:

<<http://www.computerweekly.com/Articles/2008/09/15/232308/taliban-use-skype-voip-bug-to-evade-capture.htm>>
oppure <<http://tinyurl.com/5zqlsf>>

Second Life e World of Warcraft aiutano i terroristi:

<<http://www.news.com.au/story/0,23599,22163811-2,00.html>>

Le reti wireless aperte aiutano i terroristi:

<<http://blog.wired.com/defense/2009/01/open-wi-fi-is-f.html>>
<http://www.schneier.com/blog/archives/2008/01/my_open_wireles.html>

I telefoni cellulari aiutano i terroristi:

<<http://www.foxnews.com/politics/2009/01/08/nypd-interrupt-cell-phone-service-event-terrorist-attack/>>
oppure <<http://tinyurl.com/7j9hfd>>
<<http://www.guardian.co.uk/technology/2008/dec/04/social-networking-terrorism>>
oppure <<http://tinyurl.com/5jcl3r>>
<<http://www.washingtonpost.com/wp-dyn/content/article/2009/01/31/AR2009013101548.html>>
oppure <<http://tinyurl.com/dyxmu2>>

Le automobili aiutano i terroristi:

<<http://www.guardian.co.uk/technology/2008/sep/04/terrorism.terrorismandtravel>>
oppure <<http://tinyurl.com/6hmuqs>>

I computer delle biblioteche aiutano i terroristi:

<<http://www.washingtonpost.com/wp-dyn/content/article/2005/11/04/AR2005110401030.html>>
oppure <<http://tinyurl.com/c9xyly>>

Le chat room anonime aiutano i terroristi:

<<http://query.nytimes.com/gst/fullpage.html?res=9900EEDB1230F933A15751C1A9629C8B63>>

oppure <<http://tinyurl.com/yv2mse>>

I database commerciali aiutano i terroristi:

<<http://www.computerworld.com/printthis/2005/0,4814,100161,00.html>>

La ricerca biomedica aiuta i terroristi:

<<http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2001/10/29/MN109602.DTL&type=science>>

oppure <<http://tinyurl.com/bb93zo>>

Internet abilitata sui voli di linea aiuta i terroristi:

<http://www.upi.com/Top_News/2009/02/07/In-flight_Internet_problems_foreseen/UPI-52121234029898/>

oppure <<http://tinyurl.com/dzkk76>>

Quanto ci vorrà prima che i produttori di questo dispositivo per attivare a distanza i fuochi artificiali saranno accusati di aiutare i terroristi?

<<http://www.maplin.co.uk/module.aspx?moduleno=226037>>

Questo articolo è originariamente apparso sul Guardian:

<<http://www.guardian.co.uk/technology/2009/jan/29/read-me-first-google-earth>>

oppure <<http://tinyurl.com/cjlgq6>>

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

Fuga di informazioni da Monster.com

Monster.com è stato compromesso, e sono state rubate le informazioni sensibili di molte persone. Di solito non mi prenderei nemmeno la briga di parlare di fatti del genere: succedono in continuazione. Ma un reporter dell'Associated Press mi ha chiamato per farmi rilasciare un commento. Ecco le mie parole: "L'ultima fuga di informazioni di Monster 'non avrebbe dovuto accadere', ha dichiarato Bruce Schneier, chief security officer di BT Group. 'Ma non è possibile comprendere la sicurezza di rete di un'azienda osservando solamente gli eventi pubblici, è un metro di valutazione scorretto. Tutto quel che dicono gli eventi pubblici è che sono stati attacchi abbastanza riusciti da rubare informazioni, ma non abbastanza riusciti da farlo senza lasciare traccia".

Ripensandoci, è ancora più complesso di così. Per valutare la sicurezza di rete di un'organizzazione, occorre analizzarla in modo approfondito. Non è possibile ottenere molte informazioni da attacchi abbastanza riusciti da sottrarre dati, ma non abbastanza riusciti da farlo senza lasciare traccia, e per i quali i legali della compagnia non sono stati in grado di trovare una ragione per non divulgarlo pubblicamente.

<http://www.google.com/hostednews/ap/article/ALeqM5g_bw5CTI4COJz0y50UE_ebQRfJ8QD964UTIG0>

oppure <<http://tinyurl.com/aaa8kq>>

<<http://www.telegraph.co.uk/scienceandtechnology/technology/technologynews/4370146/Hackers-steal-user-details-from-Monster.com-jobs-website.html>>

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

<http://www.usatoday.com/money/industries/technology/2009-01-27-monster-data-hackers_N.htm>

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

<<http://www.itpro.co.uk/609662/millions-of-jobseeker-details-stolen-in-monster-hack>>

oppure <<http://tinyurl.com/bx6ybr>>

<http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article5594222.ece>

oppure <<http://tinyurl.com/c4gjne>>

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

News

In dicembre, l'allora segretario del Dipartimento per la Sicurezza Nazionale Michael Chertoff ha dichiarato che i dirottamenti aerei erano una routine anche prima dell'11 settembre.

<http://www.schneier.com/blog/archives/2009/01/michael_chertof_1.html>

Elenco delle undici ragioni più importanti del perché gli elenchi dei dieci bug più notevoli non funzionano:

<<http://www.informit.com/articles/article.aspx?p=1322398>>

Ottimo articolo sul costo del temere gli sconosciuti ("The Cost of Fearing Strangers"):

<<http://freakonomics.blogs.nytimes.com/2009/01/06/the-cost-of-fearing-strangers/>>

oppure <<http://tinyurl.com/8z23ju>>

Nulla che io non abbia già detto. Ricordate, se una cosa fa notizia, non c'è ragione di preoccuparsi. La definizione stessa di "news" (le "novità", le "nuove", le notizie) è "qualcosa che capita molto raramente". È quando una cosa è talmente comune da non far più notizia (incidenti d'auto, violenza domestica) che ci si deve preoccupare.

<<http://www.schneier.com/essay-171.html>>

Frode di carta di credito eseguita di persona: il trucco sta nel convincere un commesso a telefonare a un dipendente di una compagnia di carte di credito fasulla.

<<http://www.hattiesburgamerican.com/article/20090112/NEWS01/90112029>>

Il furto di cani (o, almeno, la paura del furto di cani) è in aumento. Quindi le persone non lasciano più i propri cani legati fuori dai negozi, e acquistano guinzagli che è molto difficile tagliare.

<http://www.newyorker.com/talk/2009/01/05/090105ta_talk_julian>

Un altro documento della NSA recentemente svincolato dal segreto, sulla scoperta di TEMPEST. Risale al 1972.

<http://www.nsa.gov/public_info/files/cryptologic_spectrum/tempest.pdf>

<<http://blog.wired.com/27bstroke6/2008/04/nsa-releases-se.html>>

Un buon articolo sul perché identità, autenticazione e autorizzazione debbano rimanere distinti. Ho dedicato a questo argomento un intero capitolo di "Beyond Fear".

<<http://technet.microsoft.com/en-us/library/cc512578.aspx>>

Nel Queensland, in Australia, gli agenti di polizia stanno arrestando meno persone perché il loro nuovo sistema di immissione dei dati è troppo frustrante da utilizzare.

<<http://www.news.com.au/couriermail/story/0,23739,24723327-952,00.html>>

Questo è un bell'esempio di come incentivi non legati alla sicurezza influiscano sulle decisioni inerenti alla sicurezza.

In questa vicenda, i log di auditing di una macchina per il voto non sono serviti a capire che cosa è accaduto.

<<http://blog.wired.com/27bstroke6/2009/01/diebold-audit-1.html>>

Un lungo articolo del New York Times Magazine sulla gestione dei rischi di Wall Street e dove ha fallito. La parte più interessante spiega come gli incentivi per i trader li abbiano spinti a correre rischi asimmetrici, ossia compromessi che avrebbero avuto un buon esito nel 99% dei casi ma che avrebbero portato conseguenze catastrofiche nel rimanente 1% dei casi. Ed è esattamente quel che è accaduto.

<<http://www.nytimes.com/2009/01/04/magazine/04risk-t.html>>

Ottimi argomenti sull'insegnare la gestione dei rischi nelle scuole:

<<http://www.timesonline.co.uk/tol/news/uk/education/article5446920.ece>>

Alcuni genitori di bambini allergici alle arachidi NON stanno chiedendo alle scuole di proibire le arachidi. Considerano più importante che gli insegnanti sappiano quali bambini possano manifestare una reazione allergica e come comportarsi quando si presenta, ovvero come utilizzare un'EpiPen (iniettore di epinefrina). Questa è una risposta molto più elastica alla minaccia. Funziona anche nel caso il proibire le arachidi non fosse sufficiente. Funziona a prescindere dal fatto che il bambino manifesti una reazione anafilattica a noci, frutta, latticini, glutine, ecc. È talmente raro vedere una gestione dei rischi così razionale quando si tratta di bambini e della loro sicurezza.

<http://www.todayparent.com/shared/print.jsp?content=20080725_100226_4688>

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

Intervista affascinante con uno sviluppatore di adware.

<<http://philosecurity.org/2009/01/12/interview-with-an-adware-author>>

Ottima serie di commenti all'intervista, che dimostrano come lo sviluppatore cerchi di cambiare le carte in tavola.

<<http://www.vitalsecurity.org/2009/01/direct-revenue-twisting-history.html>>

oppure <<http://tinyurl.com/89vtrx>>

<<http://www.vitalsecurity.org/2009/01/direct-revenue-bug-not-feature.html>>

oppure <<http://tinyurl.com/a743vh>>

<<http://www.vitalsecurity.org/2009/01/we-probably-did-more-good-than-harm.html>>

oppure <<http://tinyurl.com/7xervp>>

<<http://www.vitalsecurity.org/2009/01/ignorance-is-bliss.html>>

Jeffrey Rosen sul Dipartimento per la Sicurezza Nazionale:

<<http://www.tnr.com/politics/story.html?id=5248f065-cbd3-4264-ac58-cffdfd947a22>>

oppure <<http://tinyurl.com/9vkoe6>>

Jon Stewart sulla chiusura di Guantanamo e le minacce da trama cinematografica:

<<http://www.thedailyshow.com/video/index.jhtml?videoid=216571&title=guantanamo-baywatch-the-final>>

oppure <<http://tinyurl.com/c3n7qh>>

Safe Quick Undercarriage Immobilization Device (SQUID):

<http://www.dhs.gov/xres/programs/gc_1214511688798.shtm#1>

Questa storia del Los Angeles Times, sulle linee aeree che definirebbero terrorista chiunque sia indisciplinato, sembra essere più sensazionalismo che realtà.

<http://www.latimes.com/news/nationworld/world/middleeast/la-na-airline-felonies20-2009jan20_0,28578.story>

oppure <<http://tinyurl.com/cpl9hg>>

<<http://www.popehat.com/2009/01/22/2793/>>

<<http://blog.simplejustice.us/2009/01/23/was-mommy-a-terrorist-or-la-times-full-of-it.aspx>>

oppure <<http://tinyurl.com/d74ehl>>

Studio accademico sulla valutazione dei rischi legati a eventi ad alto costo e bassa probabilità.

<<http://arxiv.org/pdf/0810.5515v1>>

Vi è un progetto di legge al Congresso (che difficilmente andrà in porto) per obbligare le fotocamere digitali a fare 'click'. L'idea di fondo è che in questo modo sarà più difficile fare fotografie di nascosto. "Il testo della proposta dice che il Congresso ha scoperto che 'bambini e adolescenti sono stati strumentalizzati mediante l'uso di fotografie scattate in spogliatoi e luoghi pubblici con la fotocamera di un cellulare'". Tutto questo è talmente idiota che ogni commento è superfluo.

<<http://arstechnica.com/tech-policy/news/2009/01/congress-gets-bill-to-make-cell-phone-cameras-go-click.ars>>

oppure <<http://tinyurl.com/bd88mq>>

Pare che in Giappone sia già legge:

<<http://news.bbc.co.uk/2/hi/asia-pacific/3031716.stm>>

Qualcuno ha effettuato un'analisi e ha calcolato il costo della no-fly list statunitense: "Come verrà analizzato poco oltre, si stima che i costi della no-fly list, dal 2002, rientrano in un intervallo compreso fra i 300 milioni di dollari circa (una stima conservativa) e i 966 milioni di dollari (una stima per eccesso). Impiegando queste cifre come potenziali valori minimo e massimo, una stima ragionevole è che il governo degli Stati Uniti abbia speso più di 500 milioni di dollari in questo progetto a partire dagli attacchi terroristici dell'11 settembre 2001. Servendosi di dati annuali, il presente articolo suggerisce che la no-fly list costi ai contribuenti una cifra compresa fra i 50 e i 161 milioni di dollari l'anno, con una media ragionevole di circa 100 milioni annui".

<<http://www.hsaj.org/?fullarticle=5.1.6>>

Le persone confessano reati che non hanno commesso. Lo fanno spesso. Quel che è interessante è che le confessioni (vere o false che siano) influenzano altri testimoni oculari.

<<http://www3.interscience.wiley.com/journal/121580382/abstract>>

<<http://www.sciam.com/podcast/episode.cfm?id=when-an-innocent-confesses-to-a-cri-09-01-27>>

oppure <<http://tinyurl.com/cxzor7>>

Una ricerca molto approfondita per corroborare la tesi secondo cui il profiling razziale non è migliore dello screening casuale:

<<http://arstechnica.com/science/news/2009/02/study-racial-profiling-no-more-effective-than-random-screen.ars>>

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

<<http://www.sciam.com/article.cfm?id=racial-profiling-terrorism-statistics>>

oppure <<http://tinyurl.com/cb98o4>>

<<http://www.nytimes.com/2009/02/03/science/03screening.html>>

<<http://www.nature.com/news/2009/090202/full/news.2009.73.html>>

La mia opinione sul profiling razziale:

<<http://www.schneier.com/blog/archives/2005/07/profiling.html>>

Esiste un nuovo standard di crittografia per i dischi rigidi, che aiuterà i costruttori a incorporare la protezione crittografica nei dischi. Onestamente, non credo sia davvero necessario. Utilizzo PGP Disk, e non ho mai notato nessun rallentamento dovuto al fatto che la crittografia è software e non hardware. E mi preoccupa veder spuntare l'ennesimo standard, con i suoi inevitabili difetti e vulnerabilità di sicurezza.

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=storage&articleId=9126869&taxonomyId=19&intsrc=kc_top>

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

<<http://arstechnica.com/hardware/news/2009/01/hard-drive-manufacturers-unveil-disk-encryption-standard.ars>>

oppure <<http://tinyurl.com/a9qn7p>>

<http://www.theregister.co.uk/2009/01/30/tcg_encryption_standards/>

Un commento molto acuto sul fatto che il vero beneficio proviene dall'osservanza delle normative:

<http://www.schneier.com/blog/archives/2009/02/hard_drive_encr.html#c347372>

oppure <<http://tinyurl.com/c8qegx>>

È facile hackerare i segnali stradali elettronici: sono dotati di lucchetti a buon mercato e la password è quella di default. Ed è divertente.

<<http://www.i-hacked.com/content/view/274/48/>>

<http://www.kxan.com/dpp/news/Road_signs_warn_of_zombies>

<<http://www.theindychannel.com/news/18620871/detail.html>>

<http://hacks.mit.edu/Hacks/by_year/2008/sign_factory/>

Questo elenco di video-corsi della NSA del 1991 è interessante, almeno per me. È più semplice seguirlo se si conoscono i vari nomi in codice e i nomi delle varie attrezzature.

<http://www.governmentattic.org/2docs/NSA_TV_Center_Catalog_1991.pdf>

Ottima vignetta di xkcd sulla differenza tra crittanalisi teorica e pratica.

<<http://xkcd.com/538/>>

Alcuni dettagli (ma non molti) sulla limousine presidenziale.

<<http://www.latimes.com/classified/automotive/highway1/la-na-inaug-car18-2009jan18,0,4020702.story>>

oppure <<http://tinyurl.com/a4h8po>>

<<http://www.msnbc.msn.com/id/28697417/>>

<<http://features.csmonitor.com/wp-content/themes/csm/popup.php?headline=Obama%26%238217%3Bs+new+limo+-+ugly+but+it+can+fend+off+asteroids&subhead=&graphic=http%3A%2F%2Ffeatures.csmonitor.com%2Fpolitics%2Fwp-content%2Fassets%2F19%2F744%2Fgraphic0.jpg>>

oppure <<http://tinyurl.com/aycpmz>>
<<http://jalopnik.com/5131380/obamas-new-cadillac-limo-officially-unveiled>>
oppure <<http://tinyurl.com/8fuvmu>>
Informazioni sul Gatling, il SUV armato che scorta la Cadillac One.
<<http://jalopnik.com/5134488/presidential-gatling-gun%20equipped-suburban-badder-than-new-cadillac-limo>>
oppure <<http://tinyurl.com/8qx3or>>

La Camera dei Rappresentanti statunitense ha approvato una proposta di legge che prevede la creazione di una lista bianca di persone che si trovano sulla lista nera no-fly, ma che non dovrebbero. Non si sa ancora che cosa faranno con gli individui che si trovano sulla lista bianca, ma che non dovrebbero. Chissà, magari creeranno un'altra lista nera per loro. Poi saremo tutti più al sicuro dai terroristi, senza dubbio.
<<http://blog.wired.com/27bstroke6/2009/02/house-approves.html>>

Un uomo è stato arrestato dalla polizia delle ferrovie Amtrak perché stava scattando fotografie per un concorso indetto dalle ferrovie Amtrak. Incredibile ma vero. Questa persona ha tolto la sua pagina Web dove parlava dell'incidente, per cui leggete il post sul mio blog per ulteriori dettagli:
<http://www.schneier.com/blog/archives/2009/02/man_arrested_by.html>
Persino Stephen Colbert ha fatto dell'ironia sull'accaduto.
<<http://www.colbertnation.com/the-colbert-report-videos/217341/february-02-2009/nailed--em---amtrak-photographer>>
oppure <<http://tinyurl.com/dy4jal>>
Non si tratta della prima volta in cui la polizia delle ferrovie Amtrak ha commesso delle idiozie.
<http://www.schneier.com/blog/archives/2008/06/filming_in_dcs.html>

Sempre sull'argomento, nel Regno Unito potrebbe presto essere illegale fotografare le forze di polizia.
<<http://www.bjp-online.com/public/showPage.html?page=836675>>

Gli SPSS (Self-Propelled Semi-Submersibles, lett. mini-sommergibili autopropulsi) vengono utilizzati per introdurre illecitamente droga negli Stati Uniti. Ma non dimentichiamoci la prospettiva terroristica: "Quel che più mi preoccupa [degli SPSS] è che se si riesce a muovere così tanta cocaina, che cos'altro si può introdurre in quei mini-sommergibili? È possibile introdurre un'arma di distruzione di massa?" ha detto l'Ammiraglio Jim Stavridis, comandante del U.S. Southern Command".
<<http://www.southcom.mil/AppsSC/factFiles.php?id=83>>

Chris Paget è in grado di clonare a distanza documenti conformi alla WHTI (Western Hemisphere Travel Initiative), come la tessera passaporto e la patente di guida EDL (Enhanced Drivers License). Non clona i passaporti, come sostengono varie fonti della stampa.
<<http://video.google.com/videoplay?docid=-282861825889939203>>
<<http://www.engadget.com/2009/02/02/video-hacker-war-drives-san-francisco-cloning-rfid-passports/>>
oppure <<http://tinyurl.com/ak67l4>>
<<http://hackaday.com/2009/02/02/mobile-rfid-scanning/>>
<<http://it.slashdot.org/article.pl?sid=09/02/04/1320223>>
<http://www.schneier.com/blog/archives/2009/02/cloning_rfid_pa_1.html>

Inquietanti cartelloni pubblicitari che... ci osservano:
<<http://www.forbes.com/feeds/ap/2009/01/31/ap5991271.html>>

Privacy su Facebook: ottimi consigli.
<<http://www.allfacebook.com/2009/02/facebook-privacy/>>

Una discussione interessante sui vari modi di 'barare' e saltare le code ai parchi divertimento Disney. Molti dei trucchi hanno a che fare con il loro sistema FastPass per la coda virtuale.
<<http://miceage.micechat.com/kevinjee/ky020309b.htm>>

Misurare il tasso di produzione delle patch per i browser a livello mondiale:
<<http://www.techzoom.net/publications/firefox-update-dynamics/index.en>>

Il Canile: i dischi rigidi Staray-S di Raidon
Pare che l'algoritmo sia lineare.
<<http://www.heise-online.co.uk/security/Cracking-budget-encryption--/features/112548>>

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

Quando si acquistano prodotti di sicurezza, occorre fidarsi del produttore. Ecco perché non compro nessuno di questi dischi con crittografia hardware. Non mi fido dei produttori.

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

La regola di esclusione delle prove e la sicurezza

Il mese scorso la Corte Suprema ha stabilito che le prove raccolte a seguito di errori presenti in un database della polizia sono ammissibili in tribunale. Questa decisione è miope e sbagliata, e farà in modo che i database delle forze dell'ordine continueranno a rimanere zeppi di errori.

I dettagli del caso sono piuttosto semplici. Secondo un database informatico, un mandato per l'arresto di Bennie Herring era in sospeso, mentre in realtà non vi era nessun mandato. Quando la polizia è andata ad arrestarlo ha effettuato una perquisizione della casa e ha scoperto una pistola e sostanze illecite. È stato quindi chiesto alla Corte Suprema di stabilire se la polizia avesse diritto o meno di arrestare Herring per il possesso di quel materiale, anche se non esistevano i fondamenti legali per giustificare la perquisizione e l'arresto in primo luogo.

Il nodo della vicenda è la regola di esclusione delle prove (exclusionary rule), che in sostanza afferma che le prove raccolte in maniera illegale o incostituzionale non sono ammissibili in tribunale. Potrà sembrare un cavillo tecnico, ma escludere quel che viene chiamato 'il frutto dell'albero avvelenato' è un sistema di sicurezza progettato per proteggere tutti noi dagli abusi della polizia.

Abbiamo una serie di leggi che limitano l'operato delle forze dell'ordine: leggi che regolamentano l'arresto, la perquisizione, l'interrogatorio, la detenzione, il processo, e così via. E uno dei modi con cui ci assicuriamo che la polizia rispetti quelle leggi è il proibire che la polizia tragga vantaggi a non rispettarle. Infatti, abbiamo ideato il

sistema in modo tale che, in effetti, sia contro gli interessi della polizia non rispettare tali leggi, perché tutte le prove che derivano dal mancato rispetto delle norme non vengono ammesse in tribunale.

E questo è ciò che fa la regola di esclusione delle prove. Se la polizia perquisisce casa vostra senza un mandato e trova della droga, non vi può arrestare per possesso illecito. Dato che le forze dell'ordine hanno di meglio da fare che buttare il proprio tempo, sono incentivate a ottenere un mandato.

Il caso Herring è più complicato, perché la polizia pensava di avere un mandato. L'errore non è stato della polizia, ma del database. E infatti il giudice Roberts ha scritto per la maggioranza: "La regola di esclusione delle prove serve a impedire una condotta premeditata, sconsiderata o grossolanamente negligente; oppure, in determinate circostanze, a frenare una negligenza ricorrente o sistematica. L'errore in questo caso non raggiunge un tale livello".

Purtroppo Roberts ha torto. I database governativi sono pieni di errori. Spesso le persone non possono visionare i dati che le riguardano e non hanno alcun modo di correggere eventuali errori o omissioni. E un numero sempre maggiore di database cerca di esentarsi dal Privacy Act del 1974, soprattutto per quanto concerne le disposizioni che richiedono precisione dei dati. La migliore argomentazione legale per escludere questo genere di prove è stata stilata da un verbale amicus curiae presentato dall'EPIC (Electronic Privacy Information Center), ma in breve il tribunale dovrebbe escludere le prove perché è l'unico sistema per garantire l'accuratezza dei database della polizia.

Ciò che ci protegge dal diventare uno stato di polizia sono i limiti imposti al potere e all'autorità delle forze dell'ordine. Non è un compromesso che accettiamo alla leggera: impediamo deliberatamente il raggio d'azione della polizia nel compimento del proprio lavoro perché riconosciamo che tali limiti ci rendono più sicuri. Senza la regola di esclusione delle prove, l'unico rimedio contro una perquisizione illegale è di fare causa alla polizia -- e ciò può essere molto arduo. Noi, la gente comune, preferiamo vedere il malcapitato in libertà piuttosto che incentivare la polizia a ignorare le leggi che limitano il suo potere.

Non applicando la regola di esclusione delle prove nel caso Herring, la Corte Suprema ha mancato un'occasione importante per spingere le forze dell'ordine a eliminare gli errori presenti nei loro database. Molti avvocati costituzionali hanno scritto parecchi articoli su questa decisione, ma l'idea più interessante proviene da Daniel J. Solove, professore alla George Washington University, che propone il seguente compromesso: "Se un determinato database è dotato di ragionevoli protezioni e misure preventive contro gli errori, allora non si dovrebbe applicare la regola di esclusione delle prove presente nel Quarto Emendamento. In caso contrario, la si applichi. Una tale regola spingerebbe i funzionari delle forze dell'ordine a mantenere database precisi, a evitare ogni genere di errori, e garantirebbe l'esistenza di una sanzione o di una simile conseguenza in caso di errore".

In misura sempre maggiore veniamo giudicati dalla scia di informazioni che ci lasciamo alle spalle. In misura sempre maggiore la precisione delle informazioni è cruciale per la nostra sicurezza e incolumità personale. E se gli errori commessi dai database della polizia da un punto di vista legale non vengono considerati alla stessa stregua degli

parte dei furti di identità avviene quando si compromette il computer di casa o dell'ufficio di un singolo individuo, non dal furto di grossi database aziendali, per cui l'effetto di queste leggi è minimo. Molti dei miglioramenti di sicurezza effettuati dalle compagnie non hanno fatto questa gran differenza, e hanno ridotto di conseguenza gli effetti di tali leggi.

Le leggi sulla notifica della perdita di informazioni fanno leva sulla pubblica umiliazione. È imbarazzante dover riconoscere la perdita o la fuga di dati, e le aziende dovrebbero essere motivate a investire in sicurezza per evitare una tale spesa di pubbliche relazioni. Il problema è che per fare in modo che questo sistema funzioni bene, l'umiliazione pubblica ha bisogno dell'appoggio della stampa. E vi è in atto un fenomeno di generale attenuazione. Il primo grande furto di informazioni dopo l'entrata in vigore della prima legge statale sulla divulgazione avvenne in California nel febbraio 2005, quando ChoicePoint vendette ai criminali informazioni private su 145.000 persone. L'evento fece scalpore, le azioni di ChoicePoint affondarono, e l'azienda fu costretta a migliorare la propria sicurezza.

In seguito, LexisNexis espose informazioni personali di 300.000 individui, e Citigroup perse i dati di 3,9 milioni di persone. La legge funzionò: l'unica ragione per cui abbiamo saputo di queste falle di sicurezza è stata grazie alla legge sulla divulgazione. Ma simili fughe di informazioni cominciarono ad accadere sempre più spesso e in quantità sempre maggiori. Le storie di questi casi sembravano sempre più un gridare 'Al lupo! Al lupo!' e molto presto le fughe di informazioni hanno smesso di fare notizia.

Oggi il costo rimanente è quello della campagna di informazione ai clienti, che spesso si rivela un'occasione per fare marketing.

Sono sempre un sostenitore di queste leggi, se non altro per le prime due ragioni che ho elencato. La divulgazione è importante, ma non è la soluzione al furto di identità. Come ho scritto in precedenza, il motivo per cui il furto di informazioni personali è così diffuso è che i dati acquistano valore una volta rubati. Il sistema per attenuare il rischio di frode per sostituzione di persona non è quello di rendere le informazioni personali più difficili da rubare -- è quello di renderle più difficili da usare.

Le leggi sulla divulgazione affrontano soltanto l'esternalità economica dei possessori dei dati che proteggono le nostre informazioni personali. Ciò di cui abbiamo davvero bisogno sono leggi che proibiscano alle istituzioni finanziarie di concedere crediti, con un livello infimo di autenticazione, a persone che si servono del nostro nome.

Lo studio della Carnegie Mellon University:

<<http://ssrn.com/abstract=1268926>>

Il mio intervento sul furto di identità:

<http://www.schneier.com/blog/archives/2005/04/mitigating_iden.html>

Questa è la seconda metà di un 'botta e risposta' con Marcus Ranum.

<http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1344729_idx2,00.html>

oppure <<http://tinyurl.com/armbx6>>

L'articolo di Marcus:

<http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1344729,00.html>

oppure <<http://tinyurl.com/d9qe77>>

** **

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>>

** **

Dal 1998 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.