

CRYPTO-GRAM
15 luglio 2007

Scritta da Bruce Schneier
Fondatore e CTO di BT Counterpane

Edizione italiana curata da Communication Valley SpA

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:

La teoria dell'inferenza corrispondente e il terrorismo

La TSA e l'incidente del bicchiere salvagoccia

News

Ubiquità della comunicazione

I diritti del Quarto Emendamento estesi alla posta elettronica

Le carte di credito e i limiti sull'acquisto di carburante

Le news su Schneier/BT Counterpane

Progettare le macchine per il voto elettronico perché riducano al minimo la coercizione

I rischi del riutilizzo dei dati

Commenti dei lettori

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

La teoria dell'inferenza corrispondente e il terrorismo

Due persone, uno sperimentatore e un soggetto, sono sedute insieme in una stanza. Lo sperimentatore si alza e va a chiudere la porta, e la stanza si fa più tranquilla. Il

soggetto molto probabilmente crederà che lo scopo dell'azione dello sperimentatore (chiudere la porta) era quello di rendere la stanza più tranquilla.

Questo è un esempio di teoria dell'inferenza corrispondente. Le persone tendono a dedurre gli scopi, e anche il temperamento, di qualcuno che svolge una certa azione basandosi sugli effetti delle sue azioni e non su fattori esterni o situazionali. Se vedete qualcuno picchiare un'altra persona con violenza, presumete che quell'individuo voleva farlo e che è una persona violenta, e non che si tratta di un attore che interpreta una parte. Se leggete la notizia di qualcuno che rimane coinvolto in un incidente d'auto, presumete che sia un pessimo conducente e non che si sia trattato di un colpo di sfortuna. E, venendo al tema di questo articolo, se leggete qualcosa che riguarda un terrorista, presumete che il suo scopo ultimo sia il terrorismo.

Naturalmente non è sempre così facile. Se un tizio decide di traslocare a Seattle invece che a New York, è per il clima, la cultura o la sua carriera? Edward Jones e Keith Davis, che promossero questa teoria negli anni Sessanta e Settanta, proposero il concetto di "corrispondenza" per descrivere il grado di preponderanza di tale effetto. Quando un'azione presenta una corrispondenza alta, le persone tendono a dedurre le intenzioni di chi agisce direttamente dall'azione stessa (esempio: colpire qualcuno con violenza). Quando un'azione presenta una corrispondenza bassa, le persone tendono a non formulare l'assunzione (esempio: traslocare a Seattle).

Come per la maggior parte dei pregiudizi cognitivi, l'inferenza corrispondente ha senso da un punto di vista evolutivo. In un mondo di azioni semplici e di obiettivi di base, è una buona regola empirica che permette a una creatura di dedurre rapidamente gli scopi di un'altra creatura ("Mi sta attaccando perché vuole uccidermi"). Anche in creature senzienti e sociali come gli esseri umani, continua ad avere senso nella maggioranza dei casi. Se vedete qualcuno colpire violentemente qualcun altro, è ragionevole assumere che si tratti di una persona violenta. I pregiudizi cognitivi non sono male: si tratta di regole empiriche sensate.

Ma come tutti i pregiudizi cognitivi, anche la teoria dell'inferenza corrispondente a volte fallisce. E un ambito in cui fallisce in maniera spettacolare è la nostra risposta al terrorismo. Dato che spesso il terrorismo ha come risultato la morte orribile di molti innocenti, noi deduciamo erroneamente che la morte orribile di molti innocenti sia la motivazione principale del terrorista o dei terroristi, e non il mezzo per uno scopo diverso.

Ho trovato quest'analisi interessante in uno studio di Max Abrahms in "International Security". "Why Terrorism Does Not Work" [Perché il terrorismo non funziona] esamina le motivazioni politiche di 28 gruppi terroristici: l'elenco completo delle "organizzazioni terroristiche straniere" delineato dal Dipartimento di Stato USA sin dal 2001. Abrahms elenca 42 obiettivi di policy di tali gruppi, e ha rilevato che i gruppi terroristici li hanno conseguiti soltanto il 7% delle volte.

Secondo i dati, il terrorismo ha più probabilità di riuscire se 1) i terroristi attaccano obiettivi militari più frequentemente che non obiettivi civili, e 2) se i terroristi hanno scopi minimalisti quali scacciare un potere straniero dal loro paese o assumere il controllo di una porzione di territorio, e non scopi massimalisti come stabilire un nuovo

sistema politico nel paese o annientare un'altra nazione. In ogni caso, il terrorismo rimane un mezzo piuttosto inefficace per influenzare una linea politica.

La metodologia di Abrahms dà adito a molte critiche sottili, ma egli sembra eccedere nell'assegnare successi ai gruppi terroristici. (Gli obiettivi degli Hezbollah di espellere sia le forze di pace sia Israele dal Libano vengono contati come un successo, e allo stesso modo viene considerato il "parziale successo" delle Tigri di Tamil di costituire uno stato Tamil). Abrahms comunque offre un'ottima serie di dati per corroborare ciò che fino a oggi tutti sapevano: che il terrorismo non funziona.

Si tratta di materiale interessante, e consiglio la lettura dello studio. Per quanto mi riguarda, la parte più sagace è quando Abrahms utilizza la teoria dell'inferenza corrispondente per spiegare perché i gruppi terroristici che attaccano soprattutto i civili non raggiungono i loro obiettivi di policy, anche se si tratta di obiettivi minimalisti. Abrahms scrive:

"Secondo la teoria qui postulata, i gruppi terroristici che prendono di mira i civili non sono in grado di forzare un cambiamento di policy perché il terrorismo presenta una corrispondenza estremamente elevata. I paesi credono che le loro popolazioni civili vengano attaccate non perché un gruppo di terroristi sta protestando contro condizioni esterne sfavorevoli, quali l'occupazione territoriale o la povertà. Le nazioni prese di mira, invece, deducono le conseguenze a breve termine dell'atto terroristico: la morte di civili innocenti, il panico di massa, la perdita di fiducia nel governo come entità protettrice, la contrazione economica e l'inevitabile erosione delle libertà civili, e le ritengono gli obiettivi dei gruppi di terroristi. In breve, i paesi presi di mira considerano le conseguenze negative degli attacchi terroristici ai danni delle loro società e sistemi politici come una prova che i terroristi vogliono distruggere quei paesi. Le nazioni bersagliate sono comprensibilmente scettiche sul fatto che il negoziare o fare concessioni piacerà ai terroristi che si ritiene siano motivati da questi obiettivi massimalisti".

In altre parole, il terrorismo non funziona perché spinge le persone a essere meno propense ad accettare le richieste dei terroristi, non importa quanto semplici o limitate esse siano. La reazione al terrorismo ha un effetto totalmente opposto a ciò che vogliono i terroristi: le persone, semplicemente, non credono che quelle richieste tanto limitate siano le richieste vere e proprie.

Questa teoria spiega, con una chiarezza mai vista prima, perché molte persone sostengano bizzarramente che il terrorismo di al Qaeda (o il terrorismo islamico in generale) sia "diverso": ovvero, che mentre altri gruppi terroristici hanno o possono avere degli obiettivi di policy, la motivazione principale di al Qaeda sia di ucciderci tutti. È una cosa che abbiamo sentito il presidente Bush affermare ripetutamente (Abrahms fa una serie di esempi nel suo studio), ed è un punto retorico nel dibattito.

Infatti gli obiettivi di policy di Bin Laden sono stati sorprendentemente coerenti finora. Abrahms ne elenca quattro; eccone sei enunciati dall'ex analista della CIA Michael Scheuer nel suo libro "Imperial Hubris":

* Terminare il supporto statunitense nei confronti di Israele

- * Spingere le truppe americane fuori dal Medioriente, specialmente dall'Arabia Saudita
- * Terminare l'occupazione USA in Afghanistan e (successivamente) in Iraq
- * Terminare il supporto degli USA delle politiche anti-musulmane di altri paesi
- * Terminare la pressione statunitense sulle compagnie petrolifere arabe affinché mantengano prezzi bassi
- * Terminare il supporto statunitense verso governi arabi "illegittimi" (cioè moderati), come il Pakistan

Anche se Bin Laden ha protestato per il fatto che gli americani hanno completamente frainteso le ragioni degli attacchi dell'11 settembre, la teoria dell'inferenza corrispondente postula che egli non sarà in grado di convincere la gente. Il terrorismo, e in special modo l'11 settembre, presentano una corrispondenza talmente elevata che le persone utilizzano gli effetti di quegli attacchi per dedurre le motivazioni dei terroristi. In altre parole, dato che Bin Laden ha provocato la morte di un paio di migliaia di persone con gli attacchi dell'11 settembre, la gente assume che questo deve essere stato il suo obiettivo, e che egli stia semplicemente presentando un'adesione formale a quelli che SOSTIENE siano i suoi obiettivi. Persino gli scopi reali di Bin Laden vengono ignorati, poiché le persone concentrano la loro attenzione sulle morti, sulla distruzione e sull'impatto economico.

Perversamente, il fraintendimento di Bush in merito agli obiettivi dei terroristi stanno efficacemente impedendo ai terroristi di raggiungere i loro scopi.

Nulla di tutto questo vuole attenuare o giustificare il terrorismo; anzi, è tutto il contrario, poiché dimostra come il terrorismo non è un buon strumento di persuasione e di cambiamento di politica. Ma potremo combattere il terrorismo in maniera più efficace se comprendiamo che si tratta di un mezzo per il raggiungimento di un fine, che non è fine a se stesso. È necessario capire le vere motivazioni dei terroristi e non solo le loro tattiche specifiche. E più i nostri pregiudizi cognitivi offuscano questa comprensione, più sbagliamo nell'identificare la minaccia, scegliendo pessimi compromessi di sicurezza.

<<http://www.mitpressjournals.org/doi/pdf/10.1162/isec.2006.31.2.42>>

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

Pregiudizi cognitivi:

<<http://www.healthbolt.net/2007/02/14/26-reasons-what-you-think-is-right-is-wrong/>>

oppure <<http://tinyurl.com/2oo5nk>>

Questo articolo è originariamente apparso su Wired.com:

<http://www.wired.com/politics/security/commentary/securitymatters/2007/07/securitymatters_0712>

oppure <<http://tinyurl.com/3y322f>>

** *** *****

La TSA e l'incidente del bicchiere salvagoccia

Questa storia è piuttosto disgustosa: "Ho richiesto di parlare con un sovrintendente della TSA [Transportation Security Administration], il quale mi ha chiesto se l'acqua nel bicchiere salvagoccia fosse 'acqua per bambini Nursery Water o un altro tipo di acqua in bottiglia'. Ho spiegato che l'acqua contenuta nel bicchiere salvagoccia era acqua del rubinetto filtrata. Il bicchiere salvagoccia mi è stato confiscato, mentre mio figlio stava piangendo e lo rivolleva, indicandolo. Ho domandato se potessi bere io l'acqua, così da poter riavere il bicchiere salvagoccia, e mi è stato detto che avrei dovuto lasciare l'area di controllo di sicurezza e ritornarvi con un bicchiere vuoto se lo volevo tenere. Mentre dei funzionari della TSA e un agente di polizia mi stavano scortando fuori dalla sicurezza, ho svitato il bicchiere per bere, e ne ho rovesciata un po', visto che ero così scossa dalla situazione.

"A questo punto sono stata trattenuta contro la mia volontà dall'agente di polizia e minacciata d'arresto per aver messo in pericolo altri passeggeri con quel poco d'acqua che avevo rovesciato. Mi è stato ordinato di asciugare il pavimento, e allora mi sono messa a pulire, inginocchiata per terra, mentre mio figlio stava seduto nel suo passeggino senza scarpe, dato che anch'esse sono state sottoposte a screening e non ho avuto tempo di rimmetterglielle. Ho chiesto di poter chiamare il mio fidanzato, che potevo ancora vedere in lontananza mentre aspettava che passassimo il checkpoint di sicurezza, così che potesse prendersi cura di mio figlio mentre io venivo trattenuta. L'agente ha minacciato di arrestarmi se mi fossi mossa. Allora ho gridato per attirare l'attenzione del mio fidanzato.

"Mi è stato ordinato di scusarmi per l'acqua rovesciata, e hanno minacciato ancora di arrestarmi. Mentre venivo trattenuta, hanno minacciato più volte di arrestarmi. Nel frattempo altri tre poliziotti sono stati chiamati a intervenire nella scena della madre con il figlio di 19 mesi. In totale, quattro agenti di polizia e tre funzionari della TSA sono intervenuti e hanno fatto rapporto mentre venivo trattenuta contro la mia volontà. Mi è anche stato detto che non avrei dovuto mancare di rispetto alle autorità e che avrei potuto essere arrestata anche per questo. Mi sono scusata con l'agente di polizia e lei ha continuato a trattenermi malgrado le stessi dicendo che avrei perso il mio volo. La sua risposta è stata che avrei dovuto pensarci prima di 'rovesciare l'acqua intenzionalmente!'"

Questa storia ritrae i funzionari della TSA come dei gorilla oppressori. La vicenda è arrivata in Internet alla metà di giugno e si è diffusa a macchia d'olio. Io l'ho vista su BoingBoing. A quanto pare, tuttavia, non è del tutto vera.

La TSA ha messo online una pagina web che riporta l'accaduto, e vi è anche un filmato.

"Il funzionario della TSA [...] ha accompagnato la donna verso la corsia di uscita, con il passeggino e la sua borsa. Quando la donna ha superato la piattaforma della corsia d'uscita, ha aperto il contenitore dell'acqua per il bambino, e ne ha platealmente rovesciato il contenuto (circa un quarto di litro) sul pavimento. L'agente della MWA

[...] stava sorvegliando la corsia d'uscita in quel momento e, osservata l'intera scena, ha avvicinato la donna e l'ha fermata mentre stava cercando di rientrare nell'area sterile dopo aver cercato di ripassare la sicurezza una volta rovesciato il liquido sul pavimento. La donna ha mostrato il suo badge e le sue credenziali e ha detto all'agente della MWA 'Lei sa chi sono io?'. È subito nata una discussione fra la donna e l'agente per stabilire se l'atto di rovesciare il liquido sia stato intenzionale o accidentale. L'agente [...] ha chiesto alla donna di asciugare per terra e lei lo ha fatto".

Guardate il secondo filmato. L'ufficiale della TSA [EMENDATO] copre parzialmente la scena, ma alle 2:01:00 PM è chiarissimo che Monica Emmerson (questo è il nome della donna) rovescia il liquido sul pavimento intenzionalmente, come un gesto deliberato di sfida. Quel che succede poi è più complicato; potete guardarlo voi stessi, o leggere il riassunto piuttosto sarcastico di BoingBoing.

In questo caso, la TSA è nettamente dalla parte della ragione.

Ma qui c'è una lezione più ampia da imparare. Vi ricordate la storia del professore di Princeton che fu inserito nella watch list per aver criticato Bush? Anche in quel caso era tutto falso. Ma perché tutti, me compreso, crediamo a queste storie? Perché siamo tutti pronti ad assumere che la TSA non è altro che una banda di gorilla oppressori, invadenti e arbitrari ed ebbri di potere?

È perché tutto sembra così arbitrario, perché non vi è alcuna responsabilità o trasparenza nel Dipartimento per la Sicurezza Nazionale. Regole e normative cambiano continuamente senza alcuna spiegazione o giustificazione. È chiaro che una cosa del genere induce paranoia. È quel genere di cose che si leggono nei libri di storia sulla Germania dell'Est ed altri stati di polizia. Non è quel che ci aspettiamo dall'America del ventesimo secolo.

Il problema è più grande della TSA, ma la TSA è la parte della "sicurezza nazionale" con cui il pubblico viene a contatto più di frequente (almeno, quella parte di pubblico che scrive soprattutto di queste cose). La TSA è il volto pubblico del problema, per cui è naturale che si prendano la maggior parte delle accuse e delle dita puntate contro.

È stata un'ottima mossa di pubbliche relazioni da parte della TSA mettere in Internet il filmato dell'incidente il più presto possibile, ma sarebbe una mossa ancora più brillante da parte del governo il ripristinare i diritti costituzionali fondamentali nella linea di condotta antiterrorismo. La responsabilità e la trasparenza sono i mattoni essenziali dell'edificio di qualsiasi democrazia; e più li perdiamo di vista, più perdiamo la nostra identità di nazione.

La storia:

<http://www.nowpublic.com/nightmare_at_reagan_national_airport_a_security_story_to_end_all_security_stories>

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

<http://www.boingboing.net/2007/06/14/tsa_detains_woman_ov.html>

La confutazione della TSA:

<http://www.tsa.gov/approach/mythbusters/dca_incident.shtm>

<http://www.boingboing.net/2007/06/15/tsa_denies_sippy_cup.html>

La storia del professore di Princeton:

<http://rawstory.com/news/2007/Professor_who_criticized_Bush_added_to_0409.html>
>

oppure <<http://tinyurl.com/yo7ljc>>

<http://blog.wired.com/27bstroke6/2007/04/debunking_the_p.html>

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

News

Rilevamento remoto di laboratori di produzione di metamfetamine: un'altra borsa di studio della NSF:

<<http://www.nsf.gov/awardsearch/showAward.do?AwardNumber=0712406>>

Un ridicolo sistema di verifica dell'età per la visione di trailer cinematografici online: "Sembra che 'Vogliamo proteggere i bambini' in realtà significhi 'Vogliamo dare l'impressione di aver fatto uno sforzo per proteggere i bambini'. Se volessero davvero proteggerli, non utilizzerebbero un sistema di autorizzazione basato sulla fiducia che l'utente indichi i dati anagrafici corretti come unica barriera che separa anteprime piene di sesso e violenza da ragazzini esperti di Internet che possono battere questo sistema inutile in pochi secondi".

<http://blogs.csoonline.com/dirty_trailers_cheap_tricks>

Il direct marketing incontra la sorveglianza all'ingrosso: una borsa di studio da 100 mila dollari della NSF:

<<http://www.nsf.gov/awardsearch/showAward.do?AwardNumber=0712287>>

Nel 1748, il pittore William Hogarth è stato arrestato e accusato di spionaggio per aver fatto degli schizzi delle fortificazioni a Calais.

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

Suona familiare, vero?

<http://www.schneier.com/blog/archives/2005/07/security_risks_3.html>

<http://www.schneier.com/blog/archives/2007/04/how_australian.html>

<<http://www.flickr.com/groups/strobist/discuss/72157600359124224/>>

Fogshield: stupida sicurezza domestica.

<http://hardwareaisle.thisoldhouse.com/2007/06/lets_smoke_em_o.html>

<http://www.schneier.com/blog/archives/2007/06/silly_home_secu.html>

Qualcuno sostiene di aver penetrato la rete della casa editrice Bloomsbury Publishing e ha pubblicato quel che sostiene essere il finale dell'ultimo libro della saga di Harry Potter. Non ci credo. Certo, è possibile, forse persino facile. Ma il testo pubblicato da questo sedicente hacker non mi convince. Da uno che è riuscito veramente a mettere le mani su una copia del manoscritto mi aspetterei che pubblicasse almeno qualche estratto del testo, non semplicemente un riassunto della trama. È più semplice e più credibile.

<<http://seclists.org/fulldisclosure/2007/Jun/0380.html>>

Il governo francese vuole vietare i dispositivi BlackBerry perché teme intercettazioni da parte dei servizi di intelligence statunitensi.

<http://www.ft.com/cms/s/dde45086-1e97-11dc-bc22-000b5df10621, i_rssPage=61e21220-6714-11da-a650-0000779e2340.html>
oppure <<http://tinyurl.com/yvka3p>>

Vulnerabilità nella rete del Dipartimento per la Sicurezza Nazionale:
<<http://blog.wired.com/27bstroke6/2007/06/dhs-security-ch.html>>

La TSA utilizza dei modelli di simulazione Monte Carlo per la stima dei rischi aerei.
<http://www.gcn.com/print/26_13/44398-1.html>

Buoni commenti al post sul mio blog:
<http://www.schneier.com/blog/archives/2007/06/tsa_uses_monte.html>

The Onion sull'apatia di una cellula terroristica:
<http://www.theonion.com/content/news/after_5_years_in_u_s_terrorist>

I "cocktail condom" sono cappucci protettivi da mettere sul proprio cocktail per evitare che qualcuno cerchi di drogare o adulterare la bevanda. Sono certo che, volendo, esistono svariati modi di battere questo dispositivo di sicurezza: una siringa, per esempio, o mettere un cappuccio nuovo dopo aver drogato il cocktail, e così via. E questo è esattamente il tipo di rischio raro che provoca reazioni eccessive. Per quanto mi riguarda, la parte più interessante della storia sono le motivazioni sottostanti. Se questi cappucci protettivi si diffonderanno con successo, non sarà per motivi di sicurezza. Sarà per la pubblicità.

<<http://abcnews.go.com/US/story?id=3302652&page=1&CMP=OTC-RSSFeeds0312>>

A qualcuno sembra vera questa storia di minacce telefoniche e di pedinamenti furtivi?
<<http://www.thenewstribune.com/front/topphoto/story/91460.html>>

<<http://consumerist.com/consumer/privacy/family-stalked-using-cellphone-snoopware-271435.php?autoplay=true>>
oppure <<http://tinyurl.com/2kk1xb>>

Qualcosa sta accadendo qui, ma mi rifiuto di credere che sia soltanto hacking dei cellulari. C'è qualcos'altro sotto.

Articolo davvero ottimo del "Washington Post" sulla segretezza:

<<http://www.washingtonpost.com/wp-dyn/content/article/2007/06/08/AR2007060802496.html>>
oppure <<http://tinyurl.com/yv7bjd>>

Nel 2002 scrissi del rapporto fra segretezza e sicurezza.

<<http://www.schneier.com/crypto-gram-0205.html#1>>

Telecamere di sorveglianza che oscurano i volti; un'interessante tecnologia a supporto della privacy.

<<http://www.technologyreview.com/Infotech/18617/>>

In spiaggia, la sabbia è più pericolosa degli squali. E questo è così importante da diventare la crociata di qualcuno?

<<http://abcnews.go.com/US/wireStory?id=3299749>>

Studio: "The only thing we have to fear is the 'culture of fear' itself" [La sola cosa che dobbiamo temere è la 'cultura della paura' stessa], di Frank Furedi.
<<http://www.frankfuredi.com/pdf/fearessay-20070404.pdf>>

Creare cartucce di stampa con inchiostro invisibile: un canale nascosto.
<<http://gizmodo.com/gadgets/clips/how-to-make-glow+in+the+dark-printer-ink-269828.php>>
oppure <<http://tinyurl.com/yoszvc>>

Bioterrorismo: sistemi di rilevamento e falsi allarmi:
<<http://www.google.com/search?q=cache:sfmQXOplWaUJ:www.the-scientist.com/article/home/52963/+>>
oppure <<http://tinyurl.com/2tjmhy>>

Pistole robotizzate:
<<http://defensenews.com/story.php?F=2803275&C=america>>

Sicurezza negli aeroporti: Israele contro gli Stati Uniti:
<<http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2007/06/17/TRGRJQF1DE1.DTL>>
oppure <<http://tinyurl.com/yqdt6f>>

Perché il PIN di uno sportello automatico ha quattro cifre:
<<http://news.bbc.co.uk/2/hi/business/6230194.stm>>

Vignetta sulla sicurezza: è sempre un compromesso:
<<http://www.gocomics.com/nonsequitur/2007/06/24>>

Osservate l'ultima frase di questo articolo, che parla di una cittadina dell'Ohio che sta pensando di rendere obbligatorie le divise nelle scuole di grado inferiore: "Per Edgewood, il motivo principale dell'adozione delle divise sarebbe quello di incrementare la sicurezza scolastica, ha dichiarato York". Di che sta parlando? Crede che le divise scolastiche incrementino la sicurezza perché sarebbe più facile notare individui che non sono studenti e che non indossano una divisa dentro e fuori la scuola? (Naturalmente i non studenti con una divisa potrebbero introdursi molto più facilmente). O si tratta di qualcos'altro? O forse oggi la sicurezza è solo una scusa per giustificare qualsiasi scempiaggine?
<<http://news.enquirer.com/apps/pbcs.dll/article?AID=/20070626/NEWS01/306260034/1056/COL02>>
oppure <<http://tinyurl.com/2yr2z8> oppure <http://tinyurl.com/253j8l>>

Ottimi commenti sulle trame terroristiche nel Regno Unito:
<http://www.theregister.co.uk/2007/06/29/more_fear_biscuits_please/>
<<http://www.theage.com.au/news/opinion/its-hard-to-prevent-the-hard-to-imagine/2007/07/02/1183351119482.html>>
oppure <<http://tinyurl.com/2dvcyv>>
<http://www.theregister.co.uk/2007/07/02/terror_idiocy_outbreak/>
<<http://www.slate.com/id/2169614/nav/tap1/>>
<http://www.atimes.com/atimes/Front_Page/IG03Aa01.html>
<http://www.theregister.co.uk/2007/07/04/ec_frattini_web_terror_dunce_cap/>

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

Nell'ex Germania dell'Est, la Stasi teneva campioni degli odori delle persone.
<<http://www.kirchersociety.org/blog/2007/04/05/smell-jars-of-the-stasi/>>

Il "Millwall brick": un'arma improvvisata fatta con un giornale, preferita dagli hooligan.
<http://en.wikipedia.org/wiki/Millwall_brick>

Quando le monete hanno più valore come metallo che come monete.
<http://news.bbc.co.uk/2/hi/south_asia/6766563.stm>

A questo tizio hanno fatto gettar via una bottiglia, ma lui l'ha ripresa dal cestino dell'immondizia e se l'è portata sull'aereo ugualmente. Non so se questo sia un atto di coraggio o di stupidità. Se fosse stato preso, la TSA gli avrebbe decisamente rovinato la giornata. Non sono nemmeno sicuro che sia una buona idea vantarsi online. Troppi idioti nell'FBI.
<http://www.zug.com/gab/index.cgi?func=view_thread&head=1&thread_id=74827>
oppure <<http://tinyurl.com/yuk2ky>>

Ho già avuto modo di parlare di questo scandalo di intercettazione avvenuto in Grecia. Si è abusato di un sistema che permette alla polizia di intercettare le conversazioni telefoniche (sorpresa, sorpresa). Questo mese a IEEE Spectrum vi è un'ottima analisi tecnica.
<<http://www.spectrum.ieee.org/print/5280>>
Commenti:
<http://www.crypto.com/blog/hellenic_eavesdropping/>
<<http://www.cs.columbia.edu/~smb/blog/2007-07/2007-07-06.html>>
<<http://mobile.nytimes.com/blogs/bits/212>>

La polizia non reagisce in modo eccessivo di fronte a uno strano oggetto. La cosa triste è che sembra quasi un'eccezione, un fatto straordinario.
<<http://www.dallasnews.com/sharedcontent/dws/dn/latestnews/stories/071007dnmetrobot.5bd61405.html>>
oppure <<http://tinyurl.com/yrys8p>>

Sono certo che la Polizia Federale Australiana ha ben chiare le proprie priorità: "La tecnologia, nella forma di umani clonati e mezzi androidi utilizzati da bande della criminalità organizzata, rappresenta la sfida futura più grande per la polizia, insieme alle truffe online, ha dichiarato il Commissario della Polizia Federale Australiana (AFP)".
<<http://www.theage.com.au/news/national/top-cop-predicts-robot-crimewave/2007/07/06/1183351416078.html>>
oppure <<http://tinyurl.com/27y45n>>

Dan Solove commenta sulla recente risoluzione ACLU contro NSA riguardante le attività di intercettazione illegali della NSA:
<http://www.concurringopinions.com/archives/2007/07/aclu_v_nsa.html>
<http://www.concurringopinions.com/archives/2007/07/aclu_v_nsa_and.html>

Dan Solove sulla privacy e sull'obiezione "non ho nulla da nascondere":
<<http://ssrn.com/abstract=998565>>

Occorre considerare il sistema del mandato come un dispositivo di sicurezza. La polizia mantiene sempre la capacità di avere accesso alla posta elettronica per indagare su un reato. Ma, per prevenire abusi, deve convincere una terza parte neutrale, un giudice, che l'accesso alle email di qualcuno è imprescindibile per investigare quel caso. Quel giudice, almeno in teoria, protegge i nostri interessi.

È ovvio che la posta elettronica merita lo stesso tipo di protezione dei nostri documenti personali, ma, come per le chiamate telefoniche, potrebbe passare molto tempo prima che i tribunali se ne rendano davvero conto. Ma ci arriveremo.

<http://blog.wired.com/27bstroke6/2007/06/appeals_court_s.html>
<<http://arstechnica.com/news.ars/post/20070619-appeals-court-feds-cant-seize-secretly-seize-e-mail-without-a-warrant.html>>
oppure <<http://tinyurl.com/26maek>>
<<http://www.freedom-to-tinker.com/?p=1170>>
<http://www.volokh.com/archives/archive_2007_06_17-2007_06_23.shtml#1182208168>
oppure <<http://tinyurl.com/yqb4uz>>
<<http://www.ca6.uscourts.gov/opinions.pdf/07a0225p-06.pdf>>

** * * * * *****

Le carte di credito e i limiti sull'acquisto di carburante

Ecco un fenomeno interessante: l'aumento dei costi del carburante ha spinto molte transazioni legittime verso il limite di guardia dell'"anti-frode".

La sicurezza è un compromesso, e ora quel tetto sta infastidendo un numero sempre più alto di conducenti che comprano benzina in modo legittimo. Ma per me il vero quesito è: questo limite, questo tetto, ha davvero un qualche scopo di sicurezza?

In generale, ai frodatori delle carte di credito piace far benzina pagando con carta, perché il sistema è automatizzato: non serve nessuna firma, e non serve interagire con altre persone. Infatti, acquistare benzina è il sistema più comune col quale un frodatore può provare la validità della carta di credito appena rubata. Il limite "anti-frode" in realtà non fa nulla per evitare tutto questo, ma riduce il quantitativo di denaro a rischio.

E con ciò? Quanti frodatori stanno davvero cercando di ottenere più benzina di quanto è permesso? Le canaglie che rubano le carte di credito stanno anche fregando automobili con serbatoi enormi, o semplicemente facendo il pieno alle auto che guidano regolarmente? Mi piacerebbe sapere quante volte, prima dell'aumento dei prezzi della benzina, il blocco innescato dal raggiungimento del limite di guardia ha coinciso davvero con la successiva denuncia di furto di una carta di credito. E qual è l'effetto di tale limite, a parte l'interruzione dell'erogazione della benzina? Di sicuro i criminali più furbi sanno che cos'è lo smurfing, nel caso abbiano bisogno di più benzina di quanto permetta il tetto massimo.

Il portavoce di Visa ha dichiarato: "Riceviamo più chiamate e domande quando aumentano i prezzi della benzina". Non ha detto "Siamo NOI A FARE PIÙ CHIAMATE per verificare un'eventuale frode". Per cui le uniche indagini a essere svolte potrebbero avvenire in quei casi in cui non sta avvenendo alcuna frode.

<<http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2007/06/15/financial/f110628D50.DTL>>
oppure <<http://tinyurl.com/ywfaqdj>>

Smurfing:

<http://en.wikipedia.org/wiki/Smurfing_%28crime%29>

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

Le news su Schneier/BT Counterpane

Slate ha scritto un articolo sul mio concorso "Minaccia da trama cinematografica".
<<http://www.slate.com/id/2169232/>>

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

Progettare le macchine per il voto elettronico perché riducano al minimo la coercizione

Se qualcuno vuole comprare il vostro voto, vorrà avere qualche prova che avete agito come d'accordo. I cellulari dotati di fotocamera sono un modo semplice per provare al compratore che avete votato come voleva lui. Le macchine per il voto elettronico in Belgio sono state progettate per minimizzare tale rischio.

"Una volta confermato il voto, lo schermo seguente non mostra come avete votato. Per cui se qualcuno viene forzato e deve produrre una prova, basta che scatti una foto del voto che è stato costretto a scegliere, quindi annullare l'operazione e cambiare voto. L'unico modo in cui a mio avviso si può aggirare il sistema è che il compratore del voto richieda un video di tutta la procedura di voto, invece di una foto della scheda".

L'autore sbaglia nel sostenere che questo sia un vantaggio che le schede elettorali elettroniche hanno rispetto a quelle cartacee. I sistemi di voto cartacei possono essere progettati con le medesime misure di sicurezza.

<<http://didierstevens.wordpress.com/2007/06/11/some-e-voting-observations/>>
oppure <<http://tinyurl.com/24k5l6>>

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

I rischi del riutilizzo dei dati

Si è saputo della cosa a marzo: contrariamente a quanto negato per decenni, lo U.S. Census Bureau ha utilizzato la documentazione sui singoli individui per calcolare il numero di cittadini americani di origine giapponese durante la Seconda Guerra Mondiale.

Normalmente, il Census Bureau non può, per legge, rivelare informazioni che possano essere collegate a singoli individui; lo scopo della legge è quello di incoraggiare le persone a rispondere alle domande del censimento con precisione e senza paura. E mentre il Second War Powers Act del 1942 sospese temporaneamente tale protezione in modo da poter localizzare i cittadini americani di origine giapponese, il Census Bureau ha sempre dichiarato di aver fornito solamente informazioni generiche su quartieri e dintorni.

Una nuova ricerca dimostra che ha mentito.

L'incidente serve per illustrare in maniera emblematica uno dei problemi più spinosi dell'era dell'informazione: i dati raccolti per uno scopo e poi utilizzati per un altro, ovvero il "riutilizzo dei dati".

Quando pensiamo ai nostri dati personali, la cosa che più ci dà fastidio, di solito, non è la raccolta e l'utilizzo iniziali, ma gli usi secondari. A me personalmente fa piacere che Amazon.com mi suggerisca libri che potrebbero interessarmi, basandosi su quelli che ho già acquistato. Mi fa piacere che la linea aerea che uso più spesso sappia dove preferisco sedermi e che cosa mi piace mangiare durante il volo, e che la mia catena di alberghi favorita registri le mie preferenze in fatto di stanze. Non mi importa che il Telepass sia collegato alla mia carta di credito e che a ogni passaggio a un casello mi venga addebitato direttamente il pedaggio. Mi piace persino il riassunto dettagliato degli acquisti che la mia compagnia di carta di credito mi invia a ogni fine anno. Quel che non voglio, però, è che una qualsiasi di queste compagnie venda le mie informazioni a dei broker; né che alle forze dell'ordine sia permesso di frugare fra i miei dati senza un mandato.

Esistono due problematiche fastidiose legate al riutilizzo dei dati. Prima di tutto, perdiamo il controllo dei nostri dati. In tutti gli esempi elencati sopra, esiste un accordo implicito fra chi raccoglie le informazioni e il sottoscritto: i dati vengono ottenuti così da potermi offrire un qualche tipo di servizio. Tuttavia, una volta che chi raccoglie quei dati li rivende a un broker, la faccenda è fuori dal mio controllo. Quelle informazioni potrebbero comparire sullo schermo di un qualche televenditore, o in un rapporto dettagliato per un potenziale datore di lavoro, o come parte di un sistema di data mining per valutare il mio livello di rischio terroristico. Diventano parte della mia ombra di dati, che sempre mi segue ma che io non posso vedere.

Ciò naturalmente va a influenzare la nostra propensione a fornire qualsiasi genere di informazione. Il motivo per cui i dati del censimento USA sono stati dichiarati intoccabili per altri scopi era quello di calmare le paure degli americani, e di rassicurarli che avrebbero potuto rispondere alle domande in modo veritiero. Quanto accurati sareste voi nel compilare il modulo del censimento se sapeste che l'FBI li utilizzerebbe per cercare dei terroristi? Come sarebbero i vostri acquisti al supermercato se sapeste che c'è qualcuno che li sta esaminando e che sta giudicando il vostro stile di vita? Conosco

molte persone che adulterano le informazioni intenzionalmente: compilano moduli dicendo menzogne per propagare dati sbagliati. Sono certo che molti di loro si comporterebbero diversamente se fossero certi che i dati venissero usati soltanto per gli scopi per cui sono stati raccolti.

La seconda problematica del riutilizzo dei dati sono i tassi di errore. Tutti i dati contengono errori, e usi diversi possono tollerare tassi di errore differenti. Quelle specie di database commerciali che si possono acquistare su Internet, per esempio, sono notoriamente zeppi di errori. Va bene: se avete appena comprato un database di cittadini americani ultra-ricchi appartenenti a una certa etnia, e il database presenta un tasso di errore del 10%, potete fattorizzarne il costo nella vostra campagna di marketing. Ma quello stesso database, con il medesimo tasso di errore, potrebbe rivelarsi del tutto inutile per le forze dell'ordine.

Comprendere i tassi di errore e come si propagano è cruciale quando si valuta un qualsiasi sistema che riutilizza i dati, specialmente se dev'essere utilizzato dalla polizia. Qualche anno fa Secure Flight, la seconda incarnazione del sistema di watch list della Transportation Security Administration, stava per utilizzare informazioni commerciali per assegnare alle persone un punteggio di rischio terroristico e determinare quanto sarebbero state interrogate o perquisite all'aeroporto. La gente si ribellò giustamente al pensiero di essere giudicata in segreto, ma vi fu un dibattito molto meno acceso per stabilire se i dati commerciali forniti dalle agenzie di credito fossero sufficientemente accurati per tale applicazione.

Un esempio ancora più eclatante dei problemi relativi ai tassi di errore è accaduto nel 2000, quando la Florida Division of Elections si impegnò insieme a Database Technologies (poi fusa con ChoicePoint) di eliminare i criminali condannati dagli elenchi elettorali. I database impiegati erano pieni di errori e le procedure di confronto approssimative, il che provocò la perdita dei diritti di voto per migliaia di persone (specie di colore), e quasi certamente cambiò il risultato di un'elezione presidenziale.

Naturalmente esistono impieghi vantaggiosi di dati secondari. Si pensi per esempio alle informazioni mediche personali. Sono dati personali, intimi, e al tempo stesso di grande valore per la società se aggregati. Si pensi a che cosa si potrebbe fare con un database contenente le informazioni sanitarie di tutti: grandi studi per determinare gli effetti a lungo termine di certi farmaci e di opzioni di trattamento, di diversi fattori ambientali, di diverse scelte di stile di vita. Nascosto in quelle informazioni vi è un'enorme quantità di potenziale di ricerca importante, e vale la pena pensare a come ottenerle senza compromettere la privacy dei singoli.

Si tratta per la maggior parte di una questione di legislazione. La tecnologia da sola non potrà mai proteggere i nostri diritti. Vi sono semplicemente troppe ragioni per non fidarsi di essa, e troppi sistemi per sovvertirla. La privacy delle informazioni alla fin fine scaturisce dalle leggi, e forti protezioni legali sono essenziali per difendere i nostri dati dagli abusi. Ma allo stesso tempo la tecnologia rimane altrettanto fondamentale.

Sia l'internamento dei giapponesi e l'epurazione degli elenchi elettorali della Florida dimostrano che le leggi possono cambiare, a volte assai rapidamente. Abbiamo bisogno di costruire sistemi dotati di tecnologie che proteggano la privacy e che limitino la raccolta di dati ove possibile. I dati che non vengono mai raccolti non possono essere

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

*** **

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

La versione italiana è curata da Communication Valley SpA

<<http://www.communicationvalley.it/>>

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

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

Per informazioni <crypto-gram@communicationvalley.it>

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

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

CRYPTO-GRAM è realizzata da Bruce Schneier. Schneier è l'autore dei best seller "Beyond Fear", "Secrets and Lies" [tradotto in Italia col titolo "Sicurezza Digitale"] e "Applied Cryptography", e inventore degli algoritmi Blowfish, Twofish e Yarrow. È il fondatore e CTO di Counterpane Internet Security, Inc., e membro del comitato consultivo dell'Electronic Privacy Information Center (EPIC). Scrive spesso e tiene conferenze in merito alla sicurezza informatica e alla 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) 2007 - Bruce Schneier.