

dappertutto. È uno dei risultati della nostra inesorabile campagna per convincere i comuni cittadini che sono loro a essere la linea del fronte della difesa antiterrorismo. "Se vedete qualcosa, dite qualcosa" recitano i cartelli nella rete metropolitana di New York. "Se sospettate qualcosa, riferitelo" invita un'altra simile campagna pubblicitaria a Manchester, Regno Unito. La polizia dello stato del Michigan ha realizzato un video di sette minuti a proposito. I funzionari dell'Amministrazione, dall'ex Procuratore Generale John Ashcroft al Segretario del Dipartimento per la Sicurezza Nazionale Michael Chertoff, allo stesso presidente Bush, ci hanno tutti chiesto di riferire qualsiasi attività sospetta.

Il problema è che i comuni cittadini non sono in grado di individuare una vera minaccia terroristica. Non sanno distinguere fra un vero ordigno esplosivo e un dispenser di nastro adesivo, un badge elettronico, un lettore di CD, un rilevatore di pipistrelli o una scultura trash; o non sanno distinguere fra terroristi cospiratori e imam, musicisti o architetti. Tutto quel che sanno è che qualcosa li mette a disagio, che sia dovuto a paura, sensazionalismo dei media, o semplicemente perché è diverso e non rientra nella "norma".

Ancora peggio è quel che accade dopo che qualcuno ha riferito una "minaccia terroristica": l'intero sistema tende all'escalation e all'atteggiamento di pararsi il didietro, invece di limitarsi a un'analisi più realistica della minaccia stessa.

Osserviamone la dinamica. Qualcuno vede qualcosa, e lo riferisce. La persona a cui lo dice (un poliziotto, una guardia di sicurezza, un assistente di volo) si trova di fronte a una scelta: ignorare o provocare un'escalation. Anche se crede si tratti di un falso allarme, scartare la minaccia non è nei suoi migliori interessi. Se ha torto, gli costerà la carriera. Ma se sceglie di provocare l'escalation, verrà elogiato per "aver fatto il suo lavoro" e il costo delle conseguenze verrà sopportato da altri. Quindi sceglie l'escalation. E anche il superiore a cui fa riferimento sceglierà l'escalation, e così via, in una serie di decisioni basate sul pararsi il didietro. E prima che il processo giunga a conclusione, verranno arrestate persone innocenti, verranno evacuati aeroporti, e le forze dell'ordine avranno sprecato centinaia di ore di lavoro.

Questa storia si è ripetuta un'infinità di volte, sia negli Stati Uniti che in altri paesi. Qualcuno (tutti fatti realmente accaduti) nota uno strano odore, o una polvere bianca, o due persone che si passano una busta, o un uomo dalla carnagione scura che lascia degli scatoloni sul cordone di un marciapiede, o un cellulare lasciato sul sedile di un aereo. La polizia delimita l'area, effettua degli arresti, e/o fa evacuare gli aerei; e alla fine la causa dell'allarme si rivela essere una ciotola di salsa chili Thai, o semplice farina, o una bolletta, o un professore inglese che sta riciclando della carta, o... un cellulare lasciato sul sedile di un aereo.

Naturalmente a quel punto è troppo tardi perché le autorità ammettano il loro errore e la loro reazione eccessiva, e che a un certo punto avrebbe dovuto prevalere un po' di buonsenso. Ciò che segue invece è una sfilata di funzionari di polizia e di funzionari eletti che si complimentano a vicenda per lo splendido lavoro portato avanti e per aver perseguito la povera vittima (la persona che era "diversa" al principio) per avere avuto l'insolenza di provare a ingannarli.

Per qualche ragione, i governi stanno incoraggiando questo tipo di comportamento. Non si tratta soltanto delle campagne pubblicitarie che invitano la gente a farsi avanti e a fare la spia; stanno chiedendo a certe professioni di prestare particolare attenzione: ai camionisti si chiede di vigilare le autostrade, agli studenti i campus, agli istruttori di subacquea i propri studenti. Gli Stati Uniti hanno chiesto agli addetti che effettuano controlli ai contatori e ai riparatori delle linee telefoniche di spiare nelle case della gente. Esiste persino una nuova legge che protegge coloro che segnalano alla polizia i propri compagni di viaggio basandosi su un non meglio specificato "sospetto oggettivamente ragionevole", qualunque esso sia.

Se si chiede a dei dilettanti di agire come personale di sicurezza di prima linea, non ci si dovrebbe

stupire se quel che si ottiene è una sicurezza di livello amatoriale.

Occorre fare due cose. La prima è di smettere di incoraggiare le persone affinché riferiscano le loro paure. La gente si è sempre fatta avanti per segnalare alla polizia situazioni genuinamente sospette, e dovrebbe continuare a farlo. Ma invitare le persone a dare l'allarme ogni volta che qualcosa le impaurisce non fa altro che sprecare le nostre risorse di sicurezza e non rende nessuno più al sicuro.

Non è che vogliamo che la gente non riferisca mai nulla. Lo scorso maggio, la soffiata dell'impiegato di un negozio ha portato alla scoperta di un complotto per attaccare Fort Dix, e in marzo, nella California del Sud, una donna molto attenta ha sventato un rapimento chiamando la polizia e segnalando un tizio sospetto che stava trasportando una cassa grande come una persona. Ma questi incidenti non fanno altro che rafforzare la necessità di valutare realisticamente le informazioni riportate dai cittadini, e non di provocare inutili escalation. Nella lotta al crimine, le forze dell'ordine hanno l'esperienza per distinguere informazioni utili e legittime dalle paure infondate, e di predisporre le risorse necessarie; dovremmo aspettarci da loro per lo meno lo stesso quando si tratta di terrorismo.

E, cosa altrettanto importante, i politici devono smetterla di elogiare e promuovere gli agenti che hanno sbagliato. E tutti devono smetterla di castigare e perseguire le vittime, colpevoli solo di aver messo in imbarazzo la polizia con la loro innocenza.

Provocare il panico in tutta una città a causa di cartelli lampeggianti, o di un tizio con una pistola ad aria compressa, o di zaini smarriti, non è affatto prova di un "ottimo lavoro". Se mai è prova di grande spreco di risorse di polizia. Ancora peggio, è fonte di una propria forma di terrore, e incoraggia la gente a essere ancor più allarmista in futuro. Dobbiamo investire le nostre risorse su cose che ci proteggano di più e sul serio, non inseguendo e strombazzando qualunque minaccia paranoica venga presentata dal primo che passa.

Le campagne pubblicitarie:

<<http://www.mta.info/mta/security/index.html>>

<http://www.manchestereveningnews.co.uk/news/s/1000/1000981_help_us_spot_terrorists_police.html>

oppure <<http://tinyurl.com/27wuan>>

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

I commenti dell'Amministrazione:

<http://www.washingtonpost.com/wp-srv/nation/attacked/transcripts/ashcroft_100801.htm>

<http://www.usatoday.com/news/washington/2005-07-07-dc-londonblasts_x.htm>

oppure <<http://tinyurl.com/25vf3y>>

<<http://query.nytimes.com/gst/fullpage.html?res=9C05E6DC1F3AF932A05752C0A9649C8B63>>

oppure <<http://tinyurl.com/2463aw>>

Incidenti:

<http://news.bbc.co.uk/1/hi/northern_ireland/6387857.stm>

<http://www.schneier.com/blog/archives/2007/09/woman_arrested.html>

<<http://www.lineofduty.com/content/view/84004/128/>>

<http://www.schneier.com/blog/archives/2007/05/uk_police_blow.html>

<<http://www.startribune.com/462/story/826056.html>>

<<http://dir.salon.com/story/tech/col/smith/2004/07/21/askthepilot95/index.html>>

oppure <<http://tinyurl.com/2bn3qo>>

<http://www.schneier.com/blog/archives/2006/10/this_is_what_vi.html>

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

<<http://www.msnbc.msn.com/id/20441775/>>

<http://www.thisisbournemouth.co.uk/display.var.1717690.0.seized_by_the_police.php>
oppure <<http://tinyurl.com/36dgj8>>
<<http://altnet.org/rights/50939/>>
<http://www.schneier.com/blog/archives/2007/04/english_profess.html>
<http://www.mercurynews.com/breakingnews/ci_7084101?nclick_check=1>
<http://www.boston.com/news/globe/city_region/breaking_news/2007/01/bomb_squad_remo.html>
oppure <<http://tinyurl.com/ywumfl>>
<<http://www.postgazette.com/pg/06081/674773.stm>>
<http://www.schneier.com/blog/archives/2007/04/another_boston.html>

Il "pararsi il didietro":

<http://www.schneier.com/blog/archives/2007/02/cya_security_1.html>

Campagne pubbliche:

<http://www.schneier.com/blog/archives/2005/12/truckers_watchi.html>
<http://www.winnipegfirst.ca/article/2007/09/24/report_suspicious_behaviour_u_of_m_tells_students>
oppure <<http://tinyurl.com/2c2t2a>>
<http://www.underwatertimes.com/print.php?article_id=64810251370>
<http://en.wikipedia.org/wiki/Operation_TIPS>

La legge che protegge i delatori:

<<http://www.post-gazette.com/pg/07245/813550-37.stm>>

"Soffiate" che hanno avuto buon esito:

<<http://www.washingtonpost.com/wp-dyn/content/article/2007/05/08/AR2007050800465.html>>
oppure <<http://tinyurl.com/38t6vd>>
<http://www.pe.com/localnews/publicsafety/stories/PE_News_Local_D_honor06.3ee3472.html>
oppure <<http://tinyurl.com/2g26xv>>

Questo articolo è originariamente apparso su Wired.com.

<http://www.wired.com/politics/security/commentary/securitymatters/2007/11/securitymatters_1101>
oppure <<http://tinyurl.com/yqvoy6>>

Alcuni link non sono stati inseriti nell'articolo originale. C'è questa agghiacciante campagna "Se vedete un padre tenere per mano suo figlio, chiamate la polizia":

<<http://www.bloggernews.net/18108>>

C'è questa storia di un iPod trovato su un aereo:

<<http://forums.worldofwarcraft.com/thread.html?topicId=11211166&pageNo=1>>

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

C'è questa storia di un "dispositivo elettronico improvvisato" che ha cercato di oltrepassare il checkpoint di sicurezza:

<http://www.makezine.com/blog/archive/2007/09/microcontroller_programme.html?CMP=OTC-0D6B48984890>

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

Questo è un ottimo articolo sulla "guerra ai dispositivi elettronici":

<http://www.cnet.com/surveillance-state/8301-13739_1-9782861-46.html>

** ** ** * * * * *

Rischi di sicurezza dei contributi politici online

il commettere qualche errore. È il discorso del libero mercato, puro e semplice, e nella maggior parte dei casi è estremamente sensato.

E le centrali chimiche sono dotate di sicurezza. Hanno recinzioni e guardie (che possono essere efficaci o meno). Sono provviste di meccanismi fail-safe incorporati nelle loro operazioni. Per esempio, molte grandi compagnie chimiche utilizzano sostanze nocive nelle loro centrali, come il fosgene, il metilisocianato e l'ossido di etilene, ma non le spediscono da un luogo all'altro. Riducono al minimo i quantitativi conservati come prodotti intermedi. In rari casi di materiali estremamente nocivi, non ne vengono conservate quantità rilevanti: sono presenti soltanto nelle condutture che collegano i reattori che li producono con i reattori che li consumano.

Tutto ciò è buono e giusto, ed è esattamente quel che detta il capitalismo basato sul libero mercato. Il problema è che non è sufficiente.

Un qualunque proprietario di una centrale chimica dotato di buonsenso proteggerà la centrale fino a non superare il valore che ha per lui. In altre parole, se la centrale vale 100 milioni di dollari, non ha senso spenderne 200 per renderla sicura. Se le probabilità che venga attaccata sono meno dell'uno per cento, non ha nemmeno senso spendere 1 milione di dollari per renderla sicura. I conti sono un po' più complessi in realtà, perché occorre tener presente cose come il costo in termini di reputazione che deriva dal trovare il proprio nome buttato in prima pagina dai media dopo un incidente, ma l'idea di fondo rimane.

Tuttavia, per la società, il costo di un attacco vero e proprio può essere molto, molto più alto. Se un terrorista fa saltare in aria una centrale particolarmente tossica nel mezzo di un'area geografica densamente popolata, i morti potrebbero essere nell'ordine delle decine di migliaia, e i danni nell'ordine di centinaia di milioni di dollari. Il danno economico indiretto potrebbe essere di miliardi di dollari. Il proprietario della centrale chimica non pagherebbe nessuno di questi costi potenziali.

Certo, il proprietario potrebbe venir denunciato. Ma non rischia più del valore della sua compagnia e, in ogni caso, correre questo rischio (la denuncia) potrebbe rivelarsi una saggia decisione. Un gruppo di costosi avvocati può fare miracoli, i tribunali possono essere volubili, e potrebbe anche intromettersi il governo e tirarlo fuori dai pasticci (come ha fatto con le linee aeree dopo l'11 settembre). E una compagnia brillante spesso può proteggersi scorporando le risorse rischiose creando una società sussidiaria, o vendendole del tutto. Il risultato generale è che le centrali chimiche del nostro paese sono molto meno protette di quel che il rischio prevederebbe.

In economia questo prende il nome di "esternalità": l'effetto di una decisione non viene sostenuto da chi ha preso la decisione. In questo caso chi ha deciso (il proprietario della centrale chimica), ha preso una decisione economica ragionevole basata sui rischi e sui costi (che riguardano soltanto lui).

Se noi (sia in quanto comunità che vive nei pressi della centrale chimica, sia in quanto intera nazione) ci aspettiamo che il proprietario di quella centrale investa denaro per aumentare la sicurezza e rendere conto di quelle esternalità, dovremo pagare per ottenerlo. E abbiamo tre modi per farlo: uno, possiamo farlo noi stessi, mettendo la polizia o l'esercito o altre entità attorno alle centrali chimiche. Due, possiamo pagare i proprietari in modo che se ne incarichino loro, sovvenzionando un qualche genere di standard di sicurezza.

O tre, potremmo instaurare delle norme di sicurezza e obbligare le aziende a pagare per conformarsi. Ovviamente non è possibile ottenere qualcosa senza pagare nulla. "Noi" come società, continuiamo a pagare in misura sempre maggiore per qualsiasi cosa stiano producendo le centrali chimiche, ma il costo viene sostenuto dai consumatori del prodotto e non dai contribuenti in generale.

<http://www.schneier.com/blog/archives/2007/10/security_risks_5.html>

Estensioni per il browser Firefox per effettuare hacking:

<http://www.darkreading.com/document.asp?doc_id=136029>

Una serie eccellente in tre parti sulle tendenze del malware criminale, incentrata soprattutto su Gozi. Malware come servizio.

<<http://www.cio.com/article/135500/>>

<<http://www.cio.com/article/135550/>>

<<http://www.cio.com/article/135551/>>

Macintosh e la sicurezza:

<http://www.macworld.com/2007/10/features/lockup_others/index.php>

Effettuare hacking ai danni del servizio di emergenza 911. Non vi sono ulteriori dettagli sulla natura di questo "hacking", né se si è trattato di qualcosa di più serio di un semplice spoofing dell'identificativo del chiamante.

<http://seattletimes.nwsourc.com/html/localnews/2003955611_hacker17.html>

oppure <<http://tinyurl.com/ytqla2>>

<<http://cwflyris.computerworld.com/t/2216044/42831165/83643/2/>>

<<http://www.msnbc.msn.com/id/21336319/>>

<<http://www.oregister.com/news/home-emami-county-1894171-ellis-system>>

Una storia affascinante di un imbroglio in un sito di poker online:

<<http://freakonomics.blogs.nytimes.com/2007/10/17/the-absolute-poker-cheating-scandal-blown-wide-open/>>

oppure <<http://tinyurl.com/2869f9>>

<<http://forumserver.twoplustwo.com/showthreaded.php?Cat=0&Number=12523924&an=&page=0&vc=1>>

oppure <<http://tinyurl.com/yuu3ts>>

<<http://forumserver.twoplustwo.com/showflat.php?Cat=0&Number=12579229&an=0&page=0#Post12579229>>

oppure <<http://tinyurl.com/23766y>>

Questo grafico che mostra il livello di rilancio sul river (la quinta carta in comune) è un'ottima prova. Si noti l'unico punto isolato in alto a destra.

<<http://www.absolutepokercheats.com/500800vpip.GIF>>

Un rapporto segreto della TSA del 2006 sulla sicurezza aeroportuale è stato fatto pervenire a USA Today (altri giornali hanno parlato della vicenda, ma i loro articoli sembrano derivare tutti dall'originale di USA Today).

<http://www.usatoday.com/printedition/news/20071018/a_insidescreeners18.art.htm>

oppure <<http://tinyurl.com/yudwy4>>

<http://www.latimes.com/news/local/la-me-airports19oct19_0,1334943.story?coll=la-home-local>

oppure <<http://tinyurl.com/2f53yv>>

<http://www.kutv.com/content/news/watercooler/story.aspx?content_id=8380cb0e-3088-4e6b-bbc4-2ca1d91754e1>

oppure <<http://tinyurl.com/2h6x8g>>

La notizia più strana: "Al San Diego International Airport i test vengono condotti da passeggeri ai quali dei responsabili locali della TSA chiedono di portare con sé un ordigno fasullo, ha affermato lo screener Chris Soulia, rappresentante in un sindacato di screener". Per favore ditemi che non è vero. "Salve Signor Passeggero. Sono un responsabile della TSA. Lei sa che non le sto mentendo per via di questo badge laminato super professionale che porto sulla giacca. Abbiamo bisogno che lei ci aiuti a collaudare la sicurezza negli aeroporti. Ecco una bomba 'fasulla' che vorremmo

mettesse nei suoi bagagli e passasse la sicurezza. Un altro responsabile della TSA la... ehm... incontrerà nel suo luogo di destinazione. Dia a lui l'ordigno fasullo quando atterra. Ah, a proposito, qual è il nome da nubile di sua madre?" Come caspita può essere questa una buona idea? Ed è così difficile travestire da turisti dei veri responsabili della TSA?

La TSA sostiene che ciò non accade:

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

La testimonianza di una persona che afferma che invece è successo, al Dulles Airport:

<<http://www.flyertalk.com/forum/showthread.php?t=737223>>

"Terroristi concettuali rivestono di marmellata la Sears Tower"

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

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

Nascondere informazioni dietro il segreto professionale nel rapporto cliente-avvocato.

<<http://denver.bizjournals.com/denver/stories/2007/09/10/story3.html>>

Ottimi commenti in merito da parte di Gregory Engel:

<<http://weblog.javazen.com/?p=528>>

Il seguente intervento, tratto dal Defcon di quest'anno, ha a che vedere con il tema.

<<http://video.google.com/videoplay?docid=1528717968000992954>>

L'utilizzo di checksum per scoprire se siete stati vittima di una frode pagando con carta di credito in un ristorante.

<<http://www.punny.org/money/fight-thieving-restaurant-servers-with-checksum-tips/>>

oppure <<http://tinyurl.com/2ga8sh>>

Non ho idea di quanto sia diffusa questa frode sulle mance. Secondo la discussione nel thread di FatWallet pare che accada piuttosto spesso, ma io uso sempre la mia carta di credito nei ristoranti di tutto il mondo e non sono mai stato vittima di questo tipo di frode. Va detto che in genere non lascio mance irrisorie. E che forse non frequento i ristoranti "giusti".

<<http://www.fatwallet.com/t/52/771939/>>

Declan McCullagh sulla politicizzazione della sicurezza:

<http://www.news.com/8301-13578_3-9795316-38.html>

Mimetizzazione urbana: voglio essere capace di travestirmi da distributore automatico di bevande.

<<http://www.nytimes.com/2007/10/20/world/asia/20japan.html?em&ex=1193198400&en=2d37e48f1fcd907c&ei=5087%0A>>

oppure <<http://tinyurl.com/29vb8k>>

<http://www.treehugger.com/files/2007/10/urban_camouflag.php>

Da piccolo realizzai il mio libro "scavato" personale. Questi sono molto più belli. Potete anche ordinare un libro "scavato" per tema, così da poterlo armonizzare al meglio con il resto della vostra biblioteca.

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

Insetti terroristi: l'ennesima minaccia da trama cinematografica di cui preoccuparsi.

<http://www.boston.com/news/globe/ideas/articles/2007/10/21/bug_bomb/>

Una scuola nel Regno Unito sta utilizzando dei chip RFID inseriti nelle uniformi scolastiche per tenere traccia delle presenze. Quindi adesso è facile marinare la scuola: basta chiedere a qualcuno di portare la nostra uniforme all'interno della struttura mentre noi ce ne stiamo altrove.

<http://www.theregister.co.uk/2007/10/22/kid_chipping_doncaster_go/>

Brandon Mayfield, il tizio dell'Oregon che è stato arrestato perché le sue impronte digitali

“coincidevano” con quelle di un algerino che ha maneggiato una delle bombe dell’attentato a Madrid, ora ha un’eredità: un giudice ha stabilito che le impronte digitali parziali non possono venire usate in un caso di omicidio.

<http://www.baltimoresun.com/news/local/baltimore_county/bal-te.md.co.prints23oct23,0,6370011.story>

oppure <<http://tinyurl.com/2vnyg8>>

Hacking ai danni di un sito Web che vende biglietti del campionato di baseball? Forse. Di certo i bagarini sono incentivati ad attaccare questo sistema.

<http://www.schneier.com/blog/archives/2007/10/world_series_ti_1.html>

Questo pedofilo pubblica foto sue in compagnia di ragazzini, ma cancella il suo viso usando il filtro “effetto spirale” di Photoshop. Risulta che la trasformazione operata dal filtro non è lossy (non c’è perdita di dati), e che è possibile applicare un effetto spirale contrario per ripristinare i suoi connotati. È stato arrestato in Thailandia. Morale: non fidarsi mai alla cieca della tecnologia; occorre sapere esattamente quel che si sta facendo.

<<http://www.boingboing.net/2007/10/08/untwirling-photo-of.html>>

<<http://www.reuters.com/article/topNews/idUSBKK21344820071019>>

La compagnia russa Elcomsoft ha effettuato il porting di un software di password cracking a una scheda video, aumentandone la velocità di 25 volte. Perché fa notizia?

<<http://technology.newscientist.com/article/dn12825-passwordcracking-chip-causes-security-concerns.html>>

oppure <<http://tinyurl.com/2sjh8v>>

<<http://blogs.techrepublic.com.com/tech-news/?p=1433&tag=nl.e019>>

AccessData, un’azienda dello Utah, ha fatto una cosa del genere per molto più tempo, e con una tecnologia migliore.

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

Dilbert e il profiling:

<<http://www.dilbert.com/comics/dilbert/archive/dilbert-20071020.html>>

<<http://www.dilbert.com/comics/dilbert/archive/dilbert-20071022.html>>

A seguito di una reazione antiterrorismo stupida quanto esagerata, i funzionari dello stato della Pennsylvania hanno deciso di non pubblicizzare l’elenco dei seggi elettorali.

<<http://www.foxnews.com/story/0,2933,305537,00.html>>

Alcuni giorni dopo, il governatore ha revocato l’ordine.

<http://www.usatoday.com/news/politics/election2008/2007-10-26-pa-polls_N.htm>

oppure <<http://tinyurl.com/yvs3vr>>

Una stampante specializzata per la stampa di patenti di guida dello stato del Missouri è stata rubata e poi recuperata. È una storia divertente. Pare che il ladro non sia riuscito ad accedere al software necessario a far funzionare la stampante. A ostacolarlo è stato un blocco del computer di controllo. Quando ha chiamato il supporto tecnico, gli addetti hanno informato i Servizi Segreti. Da una parte, un inconveniente come questo probabilmente non fermerebbe un ladro più sofisticato. Dall’altra, è possibile eseguire ottime contraffazioni con comuni attrezzature che si possono acquistare direttamente nei negozi specializzati.

<http://www.news.com/8301-10784_3-9803114-7.html>

AT&T ha un linguaggio di programmazione per la sorveglianza all’ingrosso e per il data mining:

<<http://blog.wired.com/27bstroke6/2007/10/att-invents-pro.html>>

<<http://www.freedom-to-tinker.com/?p=1219>>

La Camera dei Lords sul divieto dei liquidi sugli aerei: “Controlliamo costantemente l’efficacia delle

misure di sicurezza, in particolare quelle sui liquidi...". Come? "Il fatto che non sia accaduto nessun incidente grave legato a esplosivi liquidi indica, a mio avviso, che le contromisure instaurate finora sono state estremamente efficaci".

<http://www.theregister.co.uk/2007/10/30/lords_liquid_ban/>

Architettura e paranoia antiterrorismo:

<<http://asla.org/awards/2007/studentawards/393.html>>

<<http://www.asymmetry.org/2007/10/11/insecurity/>>

Gli spammer si servono della pornografia per rompere i captcha:

<<http://news.bbc.co.uk/1/hi/technology/7067962.stm>>

Sono anni che vado dicendo che gli spammer sarebbero arrivati a fare questo. Mi sorprende che ci abbiano messo così tanto.

Un buon articolo sull'impossibilità di scherzare su bombe e terrorismo negli aeroporti:

<<http://www.stuff.co.nz/4256682a1861.html>>

Un tizio, arrestato in quanto sospettato di omicidio, è uscito di prigione dopo essersi identificato come qualcun altro. Il sistema biometrico ha funzionato, ma l'errore umano ha prevalso. È una truffa brillante. Trovare un altro tizio arrestato, fare in modo che un amico venga a pagare la cauzione per quella persona, quindi sottrarne l'identità quando i secondini arrivano a prelevarlo.

<<http://www.cbsnews.com/stories/2007/10/29/national/main3425770.shtml>>

Il furto d'identità sintetico è destinato a diventare un problema ancor più grave del furto d'identità tradizionale:

<<http://online.wsj.com/article/SB119362045526074445.html>>

<<http://biz.yahoo.com/brn/070516/21861.html?.v=1>>

Interessante rapporto/testimonianza del GAO: "Internet Infrastructure: Challenges in Developing a Public/Private Recovery Plan" [L'infrastruttura di Internet: le sfide nello sviluppo di un piano di recupero pubblico/privato], a cura di Gregory C. Wilshusen, direttore dell'Information Security Issues, Government Accountability Office (GAO), 23 ottobre 2007.

<<http://www.gao.gov/new.items/d08212t.pdf>>

Siete arrabbiati con qualcuno? Denunciatelo come terrorista:

<http://news.yahoo.com/s/afp/20071102/od_afp/swedenjusticeterrorismoffbeat_071102124748:_ylt=Ah8e3WCMqHLBJaArTqoWc2is0NUE>

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

Lo fanno anche le aziende: "Nel maggio 2005 la richiesta della compagnia Jet di avere il permesso di volare verso l'America è stata respinta dopo che un'azienda del Maryland, anch'essa chiamata Jet Airways, aveva accusato la compagnia del signor Goyal di essere un'impresa dedita al riciclaggio di denaro per Al-Qaeda. Il signor Goyal sostiene che vi erano dei suoi concorrenti locali dietro l'accusa, che è stata successivamente ritirata".

<http://www.economist.com/people/displaystory.cfm?story_id=9762898>

Questo attacco denial-of-service contro le chiusure elettroniche delle auto è stato accidentale, ma potrebbe benissimo essere condotto di proposito.

<<http://news.bbc.co.uk/1/hi/england/kent/7073935.stm>>

Studio interessante sul furto d'identità (è lungo, ma leggete almeno il riassunto esecutivo).

<<http://www.utica.edu/academic/institutes/cimip/publications/index.cfm?action=form&paper=6>>

oppure <<http://tinyurl.com/2y225d>>

<http://www.siliconvalley.com/security/ci_7248917>

GSMK CryptoPhone G10i: è open source, e si serve di Twofish.

<<http://www.cryptophone.de/products/CPG10i/index.html>>

Una fuga di dati di Salesforce.com provoca attacchi di phishing mirati:

<<http://it.slashdot.org/article.pl?sid=07/11/06/216228>>

La storia davvero commovente di un turista straniero fatto scendere da un treno perché stava scattando fotografie:

<http://www.episcopalcafe.com/daily/war_and_peace/every_day_diplomacy.php>

oppure <<http://tinyurl.com/3x5f6c>>

La risposta dell'autore dell'articolo originale, dopo che molti avevano dubitato dell'autenticità della storia:

<http://www.schneier.com/blog/archives/2007/11/taking_pictures.html#c215790>

oppure <<http://tinyurl.com/27j8d8>>

Un attacco hacker di Al-Qaeda avrebbe dovuto aver luogo domenica scorsa. Non ho notato nulla.

<<http://www.debka.com/headline.php?hid=4723>>

Una divertente vignetta del "New Yorker" sulla sicurezza:

<http://www.cartoonbank.com/product_details.asp?sid=119416>

Attacchi suicidi nel videogioco Halo 3:

<http://www.wired.com/gaming/gamingreviews/commentary/games/2007/11/gamesfrontiers_11_05>

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

Un consulente di sicurezza informatica ammette di gestire un botnet:

<<http://www.ihf.com/articles/ap/2007/11/10/america/NA-GEN-US-Hacker-Charged.php>>

oppure <<http://tinyurl.com/yv2gy6>>

<http://blog.washingtonpost.com/securityfix/2007/11/security_pro_admits_to_hijacki.html?nav=rss_blog>

oppure <<http://tinyurl.com/246mh6>>

Una bravata durante una partita di football di liceali provoca timori di un attacco terrorista:

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

Commenti molto saggi sulla no-fly list da parte del garante della privacy canadese:

<<http://www.canada.com/edmontonjournal/news/story.html?id=4f6539d8-ccd7-4e32-a2d5-1231a6aee0a4&k=31493>>

oppure <<http://tinyurl.com/2ka3yl>>

Malcolm Gladwell sostiene in maniera convincente che il profiling dei criminali non è altro che un trucco di "cold reading":

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

Donald Kerr, il vice direttore principale della national intelligence, ha rilasciato alcuni commenti piuttosto pericolosi in merito alla ridefinizione della privacy. La stampa ha riportato soltanto quelli più "incendiari":

<http://www.cnn.com/2007/POLITICS/11/11/terrorist_surveillance.ap/index.html>

oppure <<http://tinyurl.com/ywqv2t>>

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

In realtà i suoi interventi sono più sfumati:

<http://www.odni.gov/speeches/20071023_speech.pdf>

Altri commenti:

pari di tre ordini di grandezza. Si trova nello standard solo perché è stato sostenuto dalla NSA, che lo propose per la prima volta anni fa in un progetto di standardizzazione analogo all'American National Standards Institute.

La NSA è sempre stata intimamente coinvolta negli standard crittografici statunitensi; dopotutto la sua esperienza sta proprio nel creare e nel rompere codici. Perciò la partecipazione dell'agenzia nello standard NIST non ha niente di sinistro in sé. Le questioni iniziano a presentarsi osservando più da vicino il contributo della NSA e quel che sta sotto.

I problemi con Dual_EC_DRBG furono descritti per la prima volta agli inizi del 2006. La matematica è complessa, ma in generale il problema è che i numeri casuali prodotti da questo generatore hanno una piccola predisposizione, inclinazione. Niente di così grave da rendere inutilizzabile l'algoritmo (e l'Appendice E dello standard NIST descrive un espediente per aggirare l'inghippo) ma è fonte di preoccupazione. I crittografi sono una specie conservatrice: a noi non piace utilizzare algoritmi che presentino anche il più minuscolo dei problemi.

Ma oggi la puzza di marcio intorno a Dual_EC_DRBG è ancora più pungente. Durante una presentazione informale alla conferenza CRYPTO 2007 ad agosto, Dan Shumov e Niels Ferguson hanno dimostrato che l'algoritmo contiene una debolezza che può essere descritta soltanto come una backdoor.

Ecco come funziona: vi è una serie di costanti (numeri fissi) nello standard impiegato per definire la curva ellittica dell'algoritmo. Tali costanti sono elencate nell'Appendice A della pubblicazione del NIST, ma non è spiegato da nessuna parte da dove provengono.

Quel che Shumov e Ferguson hanno dimostrato è che questi numeri si relazionano con una seconda serie segreta di numeri che può fungere da passe-partout. Se si conoscono i numeri segreti, è possibile prevedere l'output del generatore di numeri casuali dopo aver raccolto solo 32 byte dell'output stesso. Per capirci meglio con un esempio concreto, basta monitorare una sola connessione internet TLS crittografata per craccare la sicurezza di quel protocollo. Se si conoscono i numeri segreti, è possibile rompere qualsiasi istanziazione di Dual_EC_DRBG.

I ricercatori non sanno quali siano questi numeri segreti. Ma dal modo in cui funziona l'algoritmo, la persona che ha prodotto le costanti potrebbe conoscerli; egli ha avuto l'opportunità matematica di produrre le costanti e i numeri segreti in tandem.

Naturalmente non abbiamo modo di sapere se la NSA conosce o meno i numeri segreti che potrebbero compromettere Dual_EC_DRBG. Non abbiamo modo di sapere se un dipendente della NSA, lavorando per proprio conto, sia arrivato alle costanti e abbia in mano i numeri segreti. Non sappiamo se qualcuno del NIST o qualcuno del gruppo di lavoro dell'ANSI li abbia. Magari non li conosce nessuno.

Ma soprattutto non sappiamo da dove sono venute le costanti; sappiamo soltanto che chi le ha prodotte potrebbe avere la chiave per questa backdoor. E sappiamo che né il NIST, né nessun altro, possono provare altrimenti.

Tutta la questione è davvero allarmante.

Anche se nessuno è a conoscenza dei numeri segreti, il fatto che esista tale backdoor rende Dual_EC_DRBG molto fragile. Se qualcuno dovesse risolvere anche una sola istanza del problema della curva ellittica dell'algoritmo, si troverebbe in mano, per così dire, le chiavi del regno. Potrebbe sfruttarle per qualunque scopo malevolo abbia in mente, oppure potrebbe pubblicare i suoi risultati, e rendere ogni implementazione del generatore di numeri casuali totalmente insicura.

È possibile implementare Dual_EC_DRBG in maniera tale da proteggerlo contro questa backdoor, generando nuove costanti con un altro generatore di numeri casuali sicuro, e pubblicarne i seed. Questo metodo è anche menzionato nel documento del NIST, nell'Appendice A. Ma la procedura è facoltativa, e suppongo che la maggioranza delle implementazioni di Dual_EC_DRBG non si disturberà ad applicare questo accorgimento.

Se questa storia vi lascia confusi, benvenuti nel club. Non capisco perché la NSA ha insistito così tanto per includere Dual_EC_DRBG nello standard. Come trap-door non ha senso: è pubblico e piuttosto ovvio. Non ha senso da un punto di vista ingegneristico: è troppo lento perché qualcuno voglia usarlo coscientemente. E non ha senso nemmeno sotto l'aspetto della retrocompatibilità: è semplice sostituire un generatore di numeri casuali con un altro.

Il mio consiglio, se avete necessità di impiegare un generatore di numeri casuali, è di non utilizzare assolutamente Dual_EC_DRBG. Se dovete servirvi di qualcosa dello SP 800-90, usate CTR_DRBG o Hash_DRBG. O Fortuna o Yarrow, se è per questo.

Intanto, sia il NIST che la NSA hanno molte cose da spiegare.

Difetti dei generatori di numeri casuali:

- <<http://www.cs.virginia.edu/~rjg7v/annotated.html>>
- <<http://eprint.iacr.org/2007/419>>
- <<http://eprint.iacr.org/2006/086.pdf>>
- <<http://www.ddj.com/windows/184409807>>
- <<http://www.schneier.com/paper-prngs.html>>

Yarrow:

- <<http://www.schneier.com/yarrow.html>>

NIST SP 800-90:

- <http://csrc.nist.gov/publications/nistpubs/800-90/SP800-90revised_March2007.pdf>

I problemi di Dual_EC_DRBG:

- <<http://eprint.iacr.org/2006/190>>
- <<http://eprint.iacr.org/2007/048>>

La presentazioni di Shumow-Ferguson:

- <<http://rump2007.cr.yp.to/15-shumow.pdf>>

** ** ** ** **

Commenti dei lettori

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

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

** ** ** ** **

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

La versione italiana è curata da Communication Valley SpA

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

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

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

Per informazioni <crypto-gram@communicationvalley.it>

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

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

CRYPTO-GRAM è realizzata da Bruce Schneier. Schneier è l'autore dei best seller "Beyond Fear", "Secrets and Lies" [tradotto in Italia col titolo "Sicurezza Digitale"] e "Applied Cryptography", e inventore degli algoritmi Blowfish, Twofish e Yarrow. È il fondatore e CTO di 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.