

CRYPTO-GRAM  
15 settembre 2008

Scritta da Bruce Schneier  
Fondatore e CTO di BT Counterpane

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

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

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

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

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

Crypto-Gram è anche consultabile in formato RSS.

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

In questo numero:

- Nuovo libro: "Schneier on Security"
- Identity farming
- BT, Phorm, e il sottoscritto
- Il rendimento del capitale investito della Sicurezza
- Diebold ammette finalmente che le sue macchine 'perdono' voti
- News
- Divulgazione completa e l'hacking della tessera dei trasporti di Boston
- Concorso: gli anelli crittografici di Cory Doctorow
- Le news su Schneier/BT Counterpane
- I controlli di documenti d'identità con foto negli aeroporti
- Malattia mentale e omicidio
- Minacce da trama cinematografica
- Commenti dei lettori

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

Nuovo libro: "Schneier on Security"

È in uscita un mio nuovo libro: "Schneier on Security". Si tratta di una raccolta di miei articoli scritti da giugno 2002 a giugno 2008. Si trovano tutti sul mio sito Web, pertanto chi mi segue regolarmente non si perderà nulla se non acquista questo libro. Ma per chi vuole avere i miei scritti comodamente riuniti in un solo posto, o prevede di finire naufrago in un'isola deserta senza accesso Internet e vorrebbe passare il tempo

meditando sulle problematiche che di solito tratto nei miei articoli, oppure vuole regalare copie della mia opera a parenti e amici, questo libro è decisamente l'ideale. Mancano ormai tre mesi scarsi a Natale.

Il prezzo del libro con copertina rigida è di 30 dollari, ma Amazon già lo sta vendendo per 20. Se volete una copia firmata, inviatemi un'email. Vi spedirò una copia autografata per 30 dollari comprese le spese di spedizione (se negli Stati Uniti), o per 40 dollari (se la spedizione è internazionale). Sì, Amazon è più a buon mercato -- e mi si può sempre incontrare a qualche conferenza e chiedermi di autografare il libro.

Il libro:

<<http://www.schneier.com/book-sos.html>>

Gli articoli:

<<http://www.schneier.com/essays.html>>

Per ordinarlo su Amazon.com:

<<http://www.amazon.com/exec/obidos/ASIN/0470395354/counterpane/>>

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

## Identity farming

Anzitutto voglio precisare che quanto sto per dire è completamente inventato.

Immaginate di essere incaricati di immettere come infiltrati degli agenti occulti negli Stati Uniti. Siamo nel 1983, e la proliferazione di database di identità rende sempre più difficile creare delle credenziali fasulle. Dieci anni fa, chiunque nel paese avrebbe potuto farsi avanti e ottenere una patente di guida, una tessera della previdenza sociale e un conto bancario, magari servendosi dell'identità di un qualche coetaneo deceduto da bambino -- ma sta diventando sempre più arduo. E sapete che tale tendenza è destinata a continuare. Quindi decidete di 'coltivare' le vostre identità.

Chiamate questa attività "Identity farming". Inventate un gruppo di neonati. Fate richiesta per avere i loro numeri di previdenza sociale. Col tempo, aprite conti bancari a nome loro, pagate le tasse per loro, li registrate per il voto, e fate richiesta per avere carte di credito a loro nome. E adesso, 25 anni dopo, vi ritrovate con un gruppo di identità pronte e in attesa di essere 'occupate' da veri individui.

Vi sono delle complicazioni, chiaramente. Probabilmente avrete bisogno di persone che mettano firme in qualità di genitori (o almeno di madri). Probabilmente avrete bisogno di medici che compilino dei certificati di nascita. Probabilmente dovrete compilare della modulistica che certifichi che questi bambini stanno ricevendo un'istruzione privata. Di certo dovrete movimentare la loro identità finanziaria: depositando denaro nei loro conti correnti e facendo prelievi dagli sportelli Bancomat, utilizzando le loro carte di credito e pagando le bollette, e così via. E dovrete anche stabilire dei recapiti, anche se solo delle caselle postali.

Non sarete in grado di ottenere delle patenti di guida o dei documenti d'identità con foto a loro nome, però non è un grosso problema: negli Stati Uniti, più di 20 milioni di

cittadini adulti non hanno documenti del genere. Ma a parte questo, non vedo alcun motivo per cui l'identity farming non possa funzionare.

Ecco il vero interrogativo: è proprio necessario presentarsi di persona durante il corso della propria vita?

Ribadisco, mi sono inventato tutto. Non ho prove che qualcuno lo stia facendo davvero. È improbabile che una organizzazione criminale abbia interesse a farlo: venticinque anni è un traguardo troppo lontano per trarne profitti. Stesso discorso per le organizzazioni terroristiche -- non ne vale la pena. Forse ne avrebbe tratto vantaggio il KGB (anche se probabilmente sarebbe stato più difficile da giustificare dopo la caduta dell'Unione Sovietica nel 1991), e potrebbe risultare un'idea allettante per gli attuali avversari di intelligence come la Cina.

Gli immortali potrebbero servirsi di questo trucco per auto-perpetuarsi, inventandosi i propri figli e assumendone gradualmente l'identità, per poi 'ucciderne' i genitori. Potrebbero perfino presentarsi per le foto della patente di guida, mettendosi una barba finta per il ruolo del padre e una cresta di capelli blu per il ruolo del figlio. Mi è stato detto che questa è un'idea molto comune nella fan fiction di Highlander.

Lo scopo non è creare un'altra minaccia da trama cinematografica, ma di dimostrare il ruolo centrale che i dati hanno assunto nelle nostre vite. In precedenza ho sostenuto che tutti noi abbiamo un'ombra di informazioni che ci segue ovunque andiamo, e che le istituzioni interagiscono sempre più spesso con le nostre ombre di informazioni che non con noi. Incrociamo il cammino con le nostre ombre di informazioni solo ogni tanto (per esempio quando facciamo richiesta di una patente di guida o di un passaporto), e tali interazioni vengono autenticate da interazioni più vecchie e meno sicure. Il resto del mondo dà per scontato che i nostri documenti d'identità con foto ci leghino alle nostre ombre di informazioni, ignorando il collegamento piuttosto fragile fra noi e le nostre tessere di plastica (e no, REAL-ID non servirà a cambiare le cose).

A me sembra che le nostre ombre di informazioni stiano diventando sempre più delle entità distinte da noi, quasi dotate di vita propria. Quel che importa, oggi, sono le nostre ombre; noi veniamo dopo. E più la nostra società farà affidamento su queste ombre, meno saremo importanti, e potremmo persino non essere indispensabili.

Le nostre ombre di informazioni possono vivere una vita perfettamente normale senza di noi.

L'articolo sulle ombre di informazioni:  
<<http://www.schneier.com/essay-219.html>>

Un commento interessante.  
<<http://www.examiner.com/x-536-Civil-Liberties-Examiner~y2008m9d4-Im-not-myself-today-or-manufacturing-a-new-you>>  
oppure <<http://tinyurl.com/5q883m>>

Questo articolo è precedentemente apparso su Wired.com.  
<[http://www.wired.com/politics/security/commentary/securitymatters/2008/09/securitymatters\\_0904](http://www.wired.com/politics/security/commentary/securitymatters/2008/09/securitymatters_0904)>  
oppure <<http://tinyurl.com/5kmh2s>>

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

BT, Phorm, e il sottoscritto

Per tutto quest'anno ho ricevuto moltissime richieste, sia pubblicamente che privatamente, di rilasciare un commento sull'incidente tra BT e Phorm.

Non ero coinvolto con BT e Phorm, né prima né adesso. Tutto quel che so di Phorm e del rapporto fra Phorm e BT mi è giunto dagli stessi articoli che avete letto voi. Non sono coinvolto in quanto dipendente di BT, ma ogni cosa che dico è, per definizione, detta da un dirigente di BT. E non va bene.

Perciò mi spiace non poter scrivere riguardo a Phorm. Ma, onestamente, molte altre persone hanno espresso i loro punti di vista sulla questione.

<[http://www.schneier.com/blog/archives/2008/09/bt\\_phorm\\_and\\_me.html](http://www.schneier.com/blog/archives/2008/09/bt_phorm_and_me.html)>

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

Il rendimento del capitale investito della Sicurezza

Il rendimento del capitale investito (Return On Investment, o ROI) è una cosa molto importante nel business. Qualsiasi attività imprenditoriale potenzialmente rischiosa deve poter dimostrare un rendimento positivo del capitale investito, e anche un buon rendimento, per poter dare profitti.

Nell'ambito della sicurezza IT è anche diventata una cosa seria. Molti clienti a livello aziendale hanno iniziato a esigere dei modelli ROI per dimostrare che un certo investimento di sicurezza darà buoni risultati. E in risposta, i produttori stanno offrendo modelli ROI che dimostrano come la loro particolare soluzione di sicurezza fornisca il miglior rendimento del capitale investito.

In teoria si tratta di una buona idea, ma in pratica si rivela, per la maggior parte, una sciocchezza.

Prima di addentrarmi nei dettagli, voglio premettere una cosa. Il "ROI", impiegato in un contesto di sicurezza, è un termine impreciso. La sicurezza non è un investimento che dà un rendimento, come una nuova fabbrica o uno strumento finanziario. È una spesa che, se tutto va bene, ripaga perché fa risparmiare su altre spese. La sicurezza si basa sulla prevenzione delle perdite, non sui guadagni. Il termine semplicemente non ha molto senso in questo contesto.

Ma come ben sa chiunque abbia sperimentato gli esercizi di taglio del budget di fine anno di un'azienda, quando si sta cercando di far quadrare i conti, ridurre i costi equivale a far aumentare i profitti. Pertanto, malgrado la sicurezza non possa produrre ROI, la prevenzione delle perdite sicuramente va a influire sui risultati netti di una compagnia.

E una compagnia dovrebbe implementare soltanto misure di sicurezza che abbiano effetti benefici sui suoi risultati netti. Non dovrebbe spendere su un problema di sicurezza più di quanto valga il problema stesso. D'altro canto non dovrebbe ignorare quei problemi che le stanno costando un patrimonio quando esistono alternative più economiche per l'attenuazione del problema. Un'azienda intelligente deve affrontare la sicurezza come farebbe con qualsiasi altra decisione commerciale: costi e benefici.

La metodologia classica viene chiamata 'aspettativa di perdita annuale' (Annualized Loss Expectancy, o ALE), ed è molto semplice. Si calcolano i costi di un incidente di sicurezza, sia considerando fattori materiali, come tempo e denaro, sia immateriali, come reputazione e vantaggio competitivo. Si moltiplica il risultato per la probabilità che l'incidente possa accadere in un anno. Questo dovrebbe fornire la cifra da investire per mitigare il rischio. Quindi, per esempio, se il vostro negozio ha il 10 per cento di probabilità di essere rapinato e il costo di essere rapinati ammonta a 10.000 dollari, allora dovrete spendere 1.000 dollari l'anno in sicurezza. Se spendete più di quella cifra, state sciupando denaro. Se spendete meno, state sempre sciupando denaro.

Naturalmente, per essere economicamente vantaggiosi, quei mille dollari devono ridurre a zero le possibilità di essere derubati. Se una misura di sicurezza riduce la possibilità di furto del 40 per cento, fino al 6 per cento all'anno, allora non si dovrebbero investire più di 400 dollari su di essa. Se un'altra misura di sicurezza riduce la possibilità di furto dell'80%, allora vale 800 dollari. E se due misure di sicurezza riducono insieme la possibilità di essere derubati del 50%, e una costa 300 dollari e l'altra 700, allora la prima vale il denaro investito, la seconda no.

L'elemento essenziale per far funzionare tutto questo sono dei buoni dati; il termine che si utilizza è "actuarial tail", ossia un resoconto dei dati attuariali, effettivi. Se si sta effettuando un'analisi ALE di una telecamera di sicurezza in un emporio, è necessario conoscere il tasso di criminalità nella zona in cui si trova l'emporio, e magari avere anche qualche idea su quante telecamere riescano a essere un deterrente sufficiente, così da convincere i rapinatori a prendere di mira un altro negozio. Occorre conoscere quanto costa subire un furto: in termini di merce, tempo e seccature, in vendite perdute a causa di clienti spaventati, in termini di morale dei dipendenti (forse risulta difficile assumere venditori per il turno di notte). Con tutti quei dati è possibile stabilire se il costo della telecamera è inferiore alla perdita di profitti se si tiene chiuso il negozio durante la notte -- assumendo che il negozio chiuso non venga rapinato. E poi si può decidere se installarne una.

La sicurezza cibernetica è estremamente più complicata, specie perché non vi è una quantità sufficiente di dati buoni. Non esistono dei dati chiari sulla criminalità nel cyberspazio, e abbiamo molte meno informazioni su come le singole misure di sicurezza (o configurazioni specifiche di esse) attenuino tali rischi. Non abbiamo nemmeno dei dati sui costi degli incidenti.

Un problema è che la minaccia si muove troppo rapidamente. Le caratteristiche di quel che cerchiamo di prevenire cambiano così in fretta che non riusciamo ad accumulare dati con sufficiente rapidità. Quando finalmente otteniamo una certa quantità di dati, ecco apparire un nuovo modello di minaccia contro il quale non abbiamo sufficienti informazioni. Pertanto non possiamo creare dei modelli ALE.

Ma vi è un altro problema, ed è che i conti vanno presto a farsi friggere in caso di eventi rari e costosi. Immaginate di aver calcolato che i costi (in termini di reputazione,

di clienti perduti, ecc.) di vedere sui giornali il nome della vostra azienda dopo un imbarazzante incidente di sicurezza cibernetica ammontino a 20 milioni di dollari. Assumete inoltre che le probabilità che una cosa del genere avvenga in un anno sono di 1 su 10.000. Secondo l'aspettativa di perdita annuale (ALE), non dovrete investire più di 2.000 dollari per mitigare quel rischio.

Fin qui tutto bene. Ma magari il vostro CFO ritiene che un simile incidente possa costare solo 10 milioni di dollari. Non potete discutere, visto che si stanno facendo delle semplici stime. Ma lui ha appena ridotto della metà il vostro budget per la sicurezza. Un'azienda che cerca di vendervi un prodotto di sicurezza trova un'analisi sul Web che sostiene che le probabilità che un evento del genere accada sono in realtà di 1 su 1.000. Se accettate queste nuove stime, improvvisamente un prodotto che costa 10 volte di più rimane comunque un buon investimento.

Le cose si fanno peggiori quando si ha a che fare con eventi ancor più rari e costosi. Immaginate di essere incaricati dell'attenuazione del terrorismo in uno stabilimento che produce cloro. Quanto può costare alla vostra azienda un'esplosione mortale e su vasta scala, in termini monetari e di reputazione? 100 milioni di dollari? Un miliardo? 10 miliardi? E le probabilità: una su centomila, una su un milione, una su 10 milioni? A seconda di come rispondete a queste due domande (e ogni risposta in realtà è solo una supposizione) potete giustificare una spesa annua che va da 10 ai 100.000 dollari per mitigare tale rischio.

Oppure prendiamo un altro esempio: la sicurezza negli aeroporti. Assumiamo che tutte le nuove misure di sicurezza aeroportuale aumentino il tempo di attesa negli aeroporti di 30 minuti per ogni passeggero (sto inventando). Negli Stati Uniti si sono contati 760 milioni di imbarchi nel 2007. Questo significa che il tempo di attesa aggiunto negli aeroporti ci è costato un totale di 43.000 anni di tempo di attesa extra. Assumendo un'aspettativa di vita di 70 anni, il tempo di attesa in più ha 'ucciso' 620 persone all'anno (930 se si calcola il risultato basandosi su un tempo di veglia di 16 ore giornaliere). Quindi la domanda è: se abolissimo l'aumentata sicurezza aeroportuale, il numero di persone uccise dal terrorismo sarebbe maggiore o minore?

Questo genere di cose spiega perché la maggior parte di modelli ROI forniti dai produttori di sicurezza sono privi di senso. È ovvio che il loro modello dimostra come il loro prodotto o servizio sia economicamente sensato: hanno aggiustato le cifre in modo che i conti quadrino.

Ciò non significa che l'aspettativa di perdita annuale sia inutile; però è necessario 1) diffidare di ogni analisi proveniente da persone che hanno degli interessi, e 2) utilizzare i risultati solamente come linee guida generali. Perciò, quando un produttore vi mostra un modello ROI, prendetene la struttura e infilateci le vostre cifre. Non mostrate le vostre migliori al produttore: ogni cambiamento che renda il suo prodotto o servizio meno vantaggioso economicamente non verrà considerato una 'miglioria'. Quando state decidendo quali prodotti o servizi di sicurezza impiegare, utilizzate quei risultati come guida generale, unitamente alle analisi di gestione dei rischi e di fattibilità.

Articoli:

<<http://communities.intel.com/openport/blogs/it/2008/08/25/are-security-roi-figures-meaningless>>

oppure <<http://tinyurl.com/4k8agt>>

<<http://communities.intel.com/openport/blogs/it/2007/08/14/the-problem-of-measuring-information-security>>  
oppure <<http://tinyurl.com/47e8yv>>  
<https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/business/677-BSI.html>  
oppure <<http://tinyurl.com/4gyo4g>>  
<<http://taosecurity.blogspot.com/2007/07/are-questions-sound.html>>  
<<http://www.bloginfosec.com/2007/07/13/bejtlich-and-business-will-it-blend/>>  
oppure <<http://tinyurl.com/3hol5r>>  
<<http://blog.vorant.com/2007/07/my-input-to-roi-spat.html>>  
<<http://taosecurity.blogspot.com/2007/07/no-roi-no-problem.html>>  
<<http://chuvakin.blogspot.com/2007/07/security-roi-pile-up.html>>  
<<http://taosecurity.blogspot.com/2007/07/security-roi-revisited.html>>  
<<http://www.pcis.com/web/vvblog.nsf/dx/how-to-calculate-return-on-investment-roi-for-web-security>>  
oppure <<http://tinyurl.com/3elh37>>

Un esempio risibile:

<[http://www.postini.com/services/roi\\_calculator.html](http://www.postini.com/services/roi_calculator.html)>

Questo articolo è precedentemente apparso su CSO Magazine.

<[http://www.csoonline.com/article/446866/Security\\_ROI\\_Fact\\_or\\_Fiction](http://www.csoonline.com/article/446866/Security_ROI_Fact_or_Fiction)>

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

Diebold ammette finalmente che le sue macchine 'perdono' voti

Premier Election Solutions, in passato nota come Diebold Election Systems, ha finalmente ammesso che un errore vecchio di dieci anni ha causato la perdita di una quantità di voti.

Non è chiaro se tale errore sia casuale o sistematico. Se è casuale (ovvero viene persa una piccola percentuale di tutti i voti), allora è altamente improbabile che questo abbia influito sui risultati di qualsiasi elezione. Se è sistematico (ovvero viene persa una piccola percentuale di voti di un certo candidato), allora la situazione è molto più problematica.

Lo stato dell'Ohio sta tentando la denuncia.

Sempre per stare in tema, pare che a volte i funzionari elettorali si portino a casa per la notte le macchine per il voto.

<<http://www.networkworld.com/news/2008/082208-e-voting-vendor-programming-errors-caused.html>>

oppure <<http://tinyurl.com/69wzb2>>

<[http://www.theregister.co.uk/2008/08/26/decade\\_old\\_evoting\\_error/](http://www.theregister.co.uk/2008/08/26/decade_old_evoting_error/)>

<<http://www.engadget.com/2008/08/23/diebold-comes-clean-admits-that-its-e-voting-machines-are-fault/>>

oppure <<http://tinyurl.com/5fxkdp>>

<[http://voices.washingtonpost.com/trail/2008/08/21/ohio\\_voting\\_machines\\_contained.html](http://voices.washingtonpost.com/trail/2008/08/21/ohio_voting_machines_contained.html)>

oppure <<http://tinyurl.com/57ckcu>>  
<<http://www.mcclatchydc.com/election2008/story/48508.html>>

<<http://thelede.blogs.nytimes.com/2008/08/19/mom-can-my-voting-machine-spend-the-night/index.html>>

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

Il mio articolo del 2004 sulla tecnologia per le elezioni:  
<<http://www.schneier.com/crypto-gram-0411.html#1>>

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

## News

Al Cyber-Commando sperimentale, composto da 8.000 uomini, è stato ordinato di sospendere tutte le attività; questo solo alcune settimane prima di quando avrebbe dovuto essere dichiarato operativo.

<<http://blog.wired.com/defense/2008/08/air-force-suspe.html>>

L'inflazione del termine "terrorismo" continua. Deviare illegalmente un corso d'acqua è terrorismo:

<<http://www.abc.net.au/news/stories/2008/08/15/2336850.htm>>

Minacciare la gente in forma anonima usando messaggi su carte da gioco, come il Joken in "Il Cavaliere Oscuro", è terrorismo:

<[http://www.wsls.com/sls/news/local/new\\_river\\_valley/article/giles\\_county\\_teens\\_fac\\_e\\_terrorism\\_related\\_charges/15587/](http://www.wsls.com/sls/news/local/new_river_valley/article/giles_county_teens_fac_e_terrorism_related_charges/15587/)>

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

Camminare su una pista ciclabile è terrorismo:

<<http://www.timesonline.co.uk/tol/news/uk/article579334.ece>>

Ho già scritto in precedenza sulla questione:

<[http://www.schneier.com/blog/archives/2008/04/terroristic\\_thr.html](http://www.schneier.com/blog/archives/2008/04/terroristic_thr.html)>

<[http://www.schneier.com/blog/archives/2008/07/random\\_stupidit.html](http://www.schneier.com/blog/archives/2008/07/random_stupidit.html)>

L'attacco cibernetico contro la Georgia ha preceduto l'attacco vero e proprio:

<<http://www.nytimes.com/2008/08/13/technology/13cyber.html>>

Ad Shamir è stato invitato a intervenire alla conferenza Crypto 2008 con una relazione su un nuovo tipo di attacco crittanalitico chiamato "cube attack". Sostiene che il suo campo di applicazione è molto vasto: block cipher, stream cipher, funzioni hash, ecc. In generale, ogni cosa che possa essere descritta da un'equazione polinomiale di grado basso è vulnerabile: è praticamente ogni schema LFSR. L'attacco non si applica a nessun block cipher (DES, AES, Blowfish, Twofish, e così via) nell'uso comune; il loro grado è troppo elevato. (Lo studio è stato respinto da Asiacrypt, dimostrando ancora una volta come il processo di revisione della conferenza non funzioni).

<[http://www.schneier.com/blog/archives/2008/08/adi\\_shamirs\\_cub.html](http://www.schneier.com/blog/archives/2008/08/adi_shamirs_cub.html)>

<[http://www.theregister.co.uk/2008/08/26/shamir\\_cube\\_attack/](http://www.theregister.co.uk/2008/08/26/shamir_cube_attack/)>

<<http://arstechnica.com/news.ars/post/20080825-stream-ciphers-cower-before-adi-shamirs-cube-attack.html>>

oppure <<http://tinyurl.com/65fnty>>

<<http://groups.google.com/group/sci.crypt/msg/7065f9a4289581f1>>

<<http://www.mail-archive.com/cryptography@metzdowd.com/msg09686.html>>  
<<http://www.mail-archive.com/cryptography@metzdowd.com/msg09685.html>>  
Lo studio è online:  
<<http://eprint.iacr.org/2008/385>>

Una valutazione di sicurezza del protocollo Internet:  
<<http://www.cpni.gov.uk/Docs/InternetProtocol.pdf>>

Un bell'articolo del London Review of Books sulla sorveglianza personale.  
<<http://www.lrb.co.uk/v30/n16/soar01.html>>

Ah, quelli della TSA. Prima danneggiano gli aerei:  
<<http://www.aero-news.net/index.cfm?ContentBlockID=340a79d6-839a-470d-b662-944325cea23d>>  
oppure <<http://tinyurl.com/6c93ss>>  
Poi cercano di dare la colpa a qualcun altro:  
<<http://abcnews.go.com/Blotter/story?id=5624381&page=1>>  
Infastidiscono persone innocenti, ed è facile ingannarli:  
<<http://edition.cnn.com/2008/US/08/19/tsa.watch.list/index.html>>  
Come far passare degli aprilucchetti senza che la TSA se ne accorga:  
<<http://www.i-hacked.com/content/view/267/48>>

Ecco delle buone notizie in riferimento alla TSA: "Una corte di appello federale ha stabilito questa settimana che le persone bandite dai voli commerciali dalla no-fly list federale possono contestare l'arresto in una corte federale".  
<<http://arstechnica.com/news.ars/post/20080820-ruling-says-federal-courts-can-hear-no-fly-lawsuits.html>>  
oppure <<http://tinyurl.com/5drxbu>>

L'MI5 sul profiling dei terroristi: non esiste un profilo.  
<<http://www.guardian.co.uk/uk/2008/aug/20/uksecurity.terrorism1>>

Uno studio interessante: "Challenges and Directions for Monitoring P2P File Sharing Networks or Why My Printer Received a DMCA Takedown Notice" (Sfide e direzioni per il monitoraggio di reti P2P per la condivisione dei file, ovvero Perché la mia stampante ha ricevuto un avviso di arresto da parte della DMCA):  
<[http://dmca.cs.washington.edu/dmca\\_hotsec08.pdf](http://dmca.cs.washington.edu/dmca_hotsec08.pdf)>  
<<http://dmca.cs.washington.edu/>>

Le telecamere poste ai semafori per registrare infrazioni non funzionano: la soluzione a un problema ne provoca un altro:  
<[http://www.schneier.com/blog/archives/2008/08/red\\_light\\_camer.html](http://www.schneier.com/blog/archives/2008/08/red_light_camer.html)>

Come ritoccare le fotografie senza usare Photoshop: sta tutto nelle didascalie.  
<<http://morris.blogs.nytimes.com/2008/08/11/photography-as-a-weapon/>>

I computer portatili a bordo della Stazione Spaziale Internazionale sono stati infettati dal worm W32.Gammima.AG. E non è la prima volta che accade una cosa del genere.  
<<http://www.spaceref.com/news/viewnews.html?id=1305>>  
<<http://blog.wired.com/27bstroke6/2008/08/virus-infects-s.html>>  
<<http://news.bbc.co.uk/2/hi/technology/7583805.stm>>

Un aereo è stato costretto ad atterrare quando uno dei passeggeri ha avuto una reazione allergica estrema a un barattolo di zuppa di funghi il cui contenuto stava fuoriuscendo in cabina. Visto? La TSA aveva detto che i liquidi sono pericolosi.

<<http://www.examiner.ie/breaking/ireland/mhqlojkfidql/>>

Gli attacchi BGP (Border Gateway Protocol) rappresentano un grave problema. Sono attacchi di tipo man-in-the-middle. "La più grossa falla di sicurezza di Internet" (il titolo del primo link) è che ci si è sempre fidati dei collegamenti (relay) interni, anche se in realtà non sono degni di fiducia.

<<http://blog.wired.com/27bstroke6/2008/08/revealed-the-in.html>>

<<http://blog.wired.com/27bstroke6/2008/08/how-to-intercep.html>>

<<http://www.doxpara.com/?p=1231>>

Una banca inglese vieta la password di un signore:

<[http://news.bbc.co.uk/2/hi/uk\\_news/england/hereford/worcs/7585098.stm](http://news.bbc.co.uk/2/hi/uk_news/england/hereford/worcs/7585098.stm)>

Una vignetta sulle macchine per il voto elettronico. Un tipico segnale del fatto che la vostra industria ha dei problemi è quando le principali strisce a fumetti si fanno beffe di voi.

<[http://www.mycomicspage.com/features/68/feature\\_items/379490?msg\\_id=88619,379490](http://www.mycomicspage.com/features/68/feature_items/379490?msg_id=88619,379490)>

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

Un software per agevolare la frode dell'imposta sulle vendite al dettaglio:

<<http://www.nytimes.com/2008/08/30/technology/30zapper.html>>

Ecco come sottrarre informazioni dai telefoni cellulari. Morale: non date a nessuno il vostro telefono a meno che non vi fidiate di questa persona.

<[http://news.cnet.com/8301-1009\\_3-10028589-83.html](http://news.cnet.com/8301-1009_3-10028589-83.html)>

<<http://www.physorg.com/news139460365.html>>

Nel corso della storia, molti diari sono stati scritti in codice:

<[http://news.bbc.co.uk/today/hi/today/newsid\\_7586000/7586683.stm](http://news.bbc.co.uk/today/hi/today/newsid_7586000/7586683.stm)>

Un nuovo studio sulla percezione e sulla realtà delle policy sulla privacy: "What Californians Understand About Privacy Online" (Che cosa capiscono i cittadini californiani della privacy online) di Chris Jay Hoofnagle e Jennifer King.

<[http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1262130](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1262130)>

Utilizzare assegni ridotti a brandelli come materiale da imballo sembra proprio un'idea molto stupida.

<<http://consumerist.com/5040975/whh-ranch-company-uses-shredded-checks-as-package-cushioning>>

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

I calabroni effettuano dei compromessi di sicurezza:

<<http://news.bbc.co.uk/1/hi/sci/tech/7596808.stm>>

Identificare le persone mediante l'analisi della loro andatura, da telecamere poste sopra la testa e persino dai satelliti:

<[http://www.schneier.com/blog/archives/2008/09/gait\\_analysis\\_f.html](http://www.schneier.com/blog/archives/2008/09/gait_analysis_f.html)>

<<http://technology.newscientist.com/channel/tech/mg19926725.800>>

La Rock Phish Gang sta migliorando il suo software per frodi:

<[http://www.theregister.co.uk/2008/09/05/rock\\_phish\\_and\\_asprox\\_team\\_up/](http://www.theregister.co.uk/2008/09/05/rock_phish_and_asprox_team_up/)>  
<[http://www.rsa.com/blog/blog\\_entry.aspx?id=1338](http://www.rsa.com/blog/blog_entry.aspx?id=1338)>

Nella trasmissione "60 Minutes", in un'intervista con Scott Pelley, il reporter Bob Woodward ha dichiarato che l'esercito statunitense possiede una nuova tecnica segreta che è così rivoluzionaria da potersi paragonare a invenzioni come il carro armato e l'aeroplano.

<[http://www.schneier.com/blog/archives/2008/09/secret\\_military.html](http://www.schneier.com/blog/archives/2008/09/secret_military.html)>

Un episodio di "Mythbusters" sulla sicurezza del sistema RFID è stato cancellato dagli avvocati su pressione dell'industria delle carte di credito. O forse no: la persona che ha dato inizio a questa voce ha ritrattato i suoi commenti. O forse quegli stessi avvocati le hanno fatto ritrattare i commenti. Non sanno che la sicurezza ottenuta da ordini di 'imbavagliamento' non funziona mai, se non temporaneamente?

<<http://www.tomshardware.com/news/Mythbuster-RFID-HOPE,6313.html>>

<[http://news.cnet.com/8301-13772\\_3-10030509-52.html](http://news.cnet.com/8301-13772_3-10030509-52.html)>

<<http://consumerist.com/5043831/mythbusters-gagged-credit-card-companies-kill-episode-exposing-rfid-security-flaws>>

oppure <<http://tinyurl.com/56awfq>>

<[http://www.youtube.com/watch?v=-St\\_lH90Oc](http://www.youtube.com/watch?v=-St_lH90Oc)>

Un ottimo studio sulla coincidenza del DNA e il paradosso del compleanno:

<<http://freakonomics.blogs.nytimes.com/2008/08/19/are-the-fbis-probabilities-about-dna-matches-crazy/>>

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

Spegnere gli idranti in nome del terrorismo:

<[http://www.schneier.com/blog/archives/2008/09/turning\\_off\\_fir.html](http://www.schneier.com/blog/archives/2008/09/turning_off_fir.html)>

"The terrifying cost of feeling safer" (Il costo spaventoso della sensazione di sicurezza), dal Sydney Morning Herald:

<<http://business.smh.com.au/business/the-terrifying-cost-of-feeling-safer-20080826-435l.html>>

oppure <<http://tinyurl.com/4463gx>>

Il Canile: Tornado Plus, un disco USB criptato.

<<http://blogs.techrepublic.com.com/security/?p=573&tag=nl.e019>>

La NSA spia le chiamate sulla rete cellulare senza un mandato.

<[http://news.cnet.com/8301-13739\\_3-10030134-46.html](http://news.cnet.com/8301-13739_3-10030134-46.html)>

Il Ministero della Difesa del Regno Unito perde un memory stick contenente segreti militari. Non è la prima volta che è successa una cosa del genere.

<[http://news.bbc.co.uk/2/hi/uk\\_news/england/cornwall/7605923.stm](http://news.bbc.co.uk/2/hi/uk_news/england/cornwall/7605923.stm)>

Del problema in generale ho già scritto in precedenza: stiamo archiviando una quantità sempre maggiore di dati in dispositivi sempre più piccoli.

<<http://www.schneier.com/essay-105.html>>

La soluzione? Criptarli.

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

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

## Divulgazione completa e l'hacking della tessera dei trasporti di Boston

In casi straordinariamente simili in Olanda e negli Stati Uniti, i tribunali si sono recentemente trovati alle prese con la consuetudine della "divulgazione completa" tipica della sicurezza informatica, chiedendo se debba essere permesso ai ricercatori di rivelare i dettagli della vulnerabilità di una tessera dei trasporti che consente alle persone di prendere la metropolitana gratis.

La "Oyster card" utilizzata nella metropolitana di Londra è stata al centro del caso in Olanda, e una simile tessera utilizzata nella "T", la metropolitana di Boston, è stata al centro del caso negli Stati Uniti. La corte olandese ha affrontato correttamente la questione, mentre la corte americana a Boston ha sbagliato fin dal principio, malgrado si trovasse di fronte a un semplice caso di censura preventiva da Primo Emendamento.

La corte statunitense ha visto subito l'errore dei suoi metodi, ma il danno è compiuto. Ai ricercatori di sicurezza del MIT, pronti a discutere le loro scoperte nel caso di Boston alla conferenza di sicurezza DefCon, è stato vietato di intervenire.

L'etica della divulgazione totale è molto familiare per noi che ci occupiamo di sicurezza informatica. Prima che la divulgazione totale diventasse la norma, i ricercatori rivelavano le vulnerabilità in forma privata alle aziende, che le ignoravano ripetutamente. A volte i produttori arrivavano a minacciare cause legali contro i ricercatori se questi avessero divulgato le vulnerabilità.

Più avanti, i ricercatori iniziarono a rivelare l'esistenza di una certa vulnerabilità ma non i dettagli. Le aziende risposero negando l'esistenza delle falle di sicurezza, oppure definendole soltanto "teoriche". Solo quando la divulgazione completa diventò la norma, le aziende produttrici cominciarono a sistemare le vulnerabilità costantemente e velocemente. Ora che i produttori applicano periodicamente patch alle vulnerabilità, in genere i ricercatori danno loro un preavviso così che possano "patchare" i sistemi prima che la falla di sicurezza venga pubblicata. Ma anche con questo protocollo di "divulgazione responsabile", è la minaccia della divulgazione stessa che funge da incentivo affinché le aziende applichino patch ai propri sistemi. La divulgazione totale è il meccanismo grazie al quale la sicurezza informatica migliora.

Al di fuori della sicurezza informatica, la segretezza è l'atteggiamento più normale. Alcune comunità di sicurezza, come i fabbri, si comportano più come corporazioni medievali, divulgando i segreti della loro professione soltanto a chi ne fa parte. Queste comunità odiano la ricerca aperta, e hanno risposto in maniera sorprendentemente sarcastica a quei ricercatori che hanno trovato gravi vulnerabilità in lucchetti per biciclette, casseforti a combinazione, sistemi a chiave primaria, e molti altri dispositivi di sicurezza.

I ricercatori hanno ricevuto una simile reazione da altre comunità abituate più alla segretezza che all'apertura. I ricercatori -- a volte giovani studenti -- che hanno scoperto e pubblicato vulnerabilità in schemi di protezione del copyright, nella sicurezza delle macchine per il voto e ora delle schede di accesso wireless, hanno tutti subito accuse e a volte vere e proprie cause legali per non aver mantenuto segrete le falle di

sicurezza. Quando Christopher Soghoian creò un sito Web che permetteva di stampare carte d'imbarco fasulle, ricevette diverse visite sgradevoli da parte dell'FBI.

Questa preferenza per la segretezza proviene dal confondere una vulnerabilità con le informazioni che \_riguardano\_ tale vulnerabilità. Utilizzare la segretezza come misura di sicurezza è fondamentalmente fragile. Significa assumere che i criminali non svolgano le loro ricerche di sicurezza. Significa assumere che nessun altro scoprirà quella vulnerabilità. Significa assumere che non vi sarà una fuga di informazioni anche se si eliminano i risultati delle ricerche. Tutte queste presupposizioni sono sbagliate.

Il problema non sono i ricercatori, ma i prodotti stessi. Le aziende progettano la sicurezza al medesimo livello a cui giungono le esigenze dei loro clienti. La divulgazione totale aiuta i clienti a valutare la sicurezza dei prodotti che acquistano, e li educa a esigere una sicurezza migliore. La corte olandese ha perfettamente centrato la questione quando ha scritto: "I danni a NXP non provengono dalla pubblicazione dell'articolo ma dalla produzione e vendita di un chip che apparentemente presenta dei difetti".

In un mondo di segretezza forzata, i produttori rilasciano affermazioni esagerate sulle capacità dei loro prodotti, le vulnerabilità non vengono sistemate, e i clienti non ne sanno niente. La ricerca sulla sicurezza viene soffocata, e la tecnologia della sicurezza non migliora. Gli unici a beneficiarne sono i criminali.

Se perdonate l'analogia, l'etica della divulgazione totale è simile all'etica del non pagare i riscatti nei casi di sequestro. Tutti sappiamo perché i sequestratori non devono essere pagati: sarebbe un incentivo a compiere altri rapimenti. Eppure in ogni caso di sequestro c'è sempre qualcuno (un coniuge, un parente, un datore di lavoro) con un'ottima ragione per cui, solo in questo caso specifico, dovremmo fare un'eccezione.

Il motivo per cui vogliamo che i ricercatori pubblichino le vulnerabilità è perché in questo modo la sicurezza migliora. Ma in ogni caso c'è sempre qualcuno (la Massachusetts Bay Transit Authority, i fabbri, un costruttore di macchine per il voto) a sostenere che, solo in questo caso specifico, dovremmo fare un'eccezione.

Invece non dobbiamo. I benefici della pubblicazione responsabile degli attacchi superano di molto i danni potenziali. La divulgazione e la trasparenza incoraggiano le compagnie a creare sicurezza in modo appropriato invece di affidarsi a progetti malfatti e alla segretezza, e le scoraggiano a promettere sicurezza basata sulla loro capacità di minacciare i ricercatori. È in questo modo che si conosce la sicurezza e si migliora la sicurezza futura.

<<http://blog.wired.com/27bstroke6/2008/08/eff-to-appeal-r.html>>

La Oyster Card di Londra:

<<http://www.schneier.com/essay-229.html>>

<[http://zoeken.rechtspraak.nl/resultpage.aspx?snelzoeken=true&searchtype=ljn&ljn=BD7578&u\\_ljn=BD7578](http://zoeken.rechtspraak.nl/resultpage.aspx?snelzoeken=true&searchtype=ljn&ljn=BD7578&u_ljn=BD7578)>

oppure <<http://tinyurl.com/43vqp8>>

La tessera dei trasporti di Boston:

<<http://blog.wired.com/27bstroke6/2008/08/computer-scient.html>>

<<http://blog.wired.com/27bstroke6/2008/08/injunction-requ.html>>

<<http://blog.wired.com/27bstroke6/2008/08/federal-judge-t.html>>  
<<http://www.groklaw.net/article.php?story=20080819142913408>>

Divulgazione totale:

<<http://www.schneier.com/essay-146.html>>  
<<http://www.schneier.com/crypto-gram-0111.html#1>>  
<[http://www.eff.org/files/filenode/MBTA\\_v\\_Anderson/letter081208.pdf](http://www.eff.org/files/filenode/MBTA_v_Anderson/letter081208.pdf)>

I fabbrici e la divulgazione totale:

<[http://news.cnet.com/8301-1009\\_3-10002138-83.html?tag=mncol](http://news.cnet.com/8301-1009_3-10002138-83.html?tag=mncol)>  
<<http://www.slate.com/id/2195862/>>  
<<http://www.theglobeandmail.com/servlet/story/RTGAM.20080711.wlpicking11/EmailBNStory/lifeMain/>>  
oppure <<http://tinyurl.com/6mm7qv>>  
<<http://www.schneier.com/crypto-gram-0302.html#1>>  
<<http://www.crypto.com/papers/kiss.html>>  
<<http://www.crypto.com/papers/flattery.html>>  
<<http://www.wired.com/culture/lifestyle/news/2004/09/64987>>  
<<http://www.crypto.com/papers/safelocks.pdf>>  
<<http://www.crypto.com/masterkey.html>>  
<<http://blog.wired.com/27bstroke6/2008/08/medeco-locks-cr.html>>  
<[http://en.wikipedia.org/wiki/Lock\\_bumping](http://en.wikipedia.org/wiki/Lock_bumping)>

Altre reazioni alla divulgazione totale:

<<http://compsci.ca/blog/lanschul-threatens-compscica-with-legal-actions/>>  
oppure <<http://tinyurl.com/3pbvrv>>  
<<http://www.freedom-to-tinker.com/?p=1265>>  
<[http://www.schneier.com/blog/archives/2006/11/forge\\_your\\_own.html](http://www.schneier.com/blog/archives/2006/11/forge_your_own.html)>

Segretezza e sicurezza:

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

Matt Blaze ha un ottimo commento sull'argomento.

<[http://www.crypto.com/blog/security\\_through\\_restraining\\_orders/](http://www.crypto.com/blog/security_through_restraining_orders/)>

Questo articolo è precedentemente apparso su Wired.com.

<[http://www.wired.com/politics/security/commentary/securitymatters/2008/08/securitymatters\\_0821](http://www.wired.com/politics/security/commentary/securitymatters/2008/08/securitymatters_0821)>  
oppure <<http://tinyurl.com/5beqak>>

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

Concorso: gli anelli crittografici di Cory Doctorow

Cory Doctorow voleva un anello di matrimonio con un decoder crittografico e mi ha chiesto aiuto per progettarglielo. Volevo qualcosa in più del solito anello crittografico, quindi la mia richiesta è stata la seguente: "Voglio che ogni rotella sia l'alfabeto, e che ogni lettera abbia o un puntino sopra di essa, o un puntino sotto di essa, oppure nessun puntino. La prima rotella dovrebbe alternare la posizione 'sopra', 'nessuno', 'sotto'. La seconda rotella dovrebbe avere una sequenza ricorrente di 'sopra', 'sopra', 'nessuno',

'nessuno', 'sotto', 'sotto'. La terza rotella dovrebbe avere una sequenza ricorrente di 'sopra', 'sopra', 'sopra', 'nessuno', 'nessuno', 'nessuno', 'sotto', 'sotto', 'sotto'. (So che suona un po' confuso; osservate la figura).

Pertanto questo è ciò che Cory ha chiesto, e questo ha ottenuto. E ora è venuto il momento di creare qualche applicazione crittografica per gli anelli. Cory ed io abbiamo lanciato un concorso aperto per trovare l'applicazione più brillante.

Non credo che possiamo inventare alcun algoritmo crittografico che possa resistere all'analisi computerizzata (non vi è sufficiente entropia nel sistema), ma possiamo scovare qualche buon cifrato tradizionale 'carta e matita' che sarà utile agli sposini se mai si troveranno prigionieri nel passato. Ed esistono di sicuro molti altri impieghi per gli anelli.

Ecco un sistema per utilizzare gli anelli per ricordare le password. Anzitutto si sceglie una chiave a due lettere. Allineate le tre rotelle secondo questa chiave. Per esempio, se la chiave è 'EB' per eBay, allineare le tre lettere AEB. Prendete la classica password 'PASSWORD' e criptatela. Per ogni lettera, trovatela sulla rotella superiore. Contate una lettera a sinistra se vi è un puntino sopra la lettera, e una lettera a destra se vi è un puntino sotto di essa. Prendete quella nuova lettera e guardate quale altra lettera si trova sotto di essa (nella rotella centrale). Contate due lettere a sinistra se vi è un puntino su di essa, e due lettere a destra se il puntino è sotto di essa. Prendete quella nuova lettera (nella rotella centrale) e guardate quale altra lettera si trova sotto di essa (nella rotella inferiore). Contate tre lettere a sinistra se vi è un puntino su di essa, e tre lettere a destra se il puntino è sotto di essa. Quella sarà la lettera cifrata. Fatelo con ogni lettera per ottenere la password.

'PASSWORD' e la chiave 'EB' diventa 'NXPPVVOF'.

Non è un granché; qualcuno sa spiegare perché? (Ignorate per ora il fatto che pubblicare il procedimento su un blog faccia perdere sicurezza al sistema).

Come si può migliorare quella tecnica? Che cos'altro si può fare con gli anelli? Possiamo incorporare altri elementi, come un mazzo di carte del Solitario, o monete di diverse dimensioni, per rendere il sistema più sicuro?

Inviare le vostre proposte in forma di commenti nel blog di Cory o inviatele all'indirizzo [cryptocontest@craphound.com](mailto:cryptocontest@craphound.com). La scadenza è il primo di ottobre.

Buona fortuna e buon divertimento.

Gli anelli crittografici:

<[http://en.wikipedia.org/wiki/Secret\\_decoder\\_ring](http://en.wikipedia.org/wiki/Secret_decoder_ring)>

Foto e schema:

<<http://www.flickr.com/photos/doctorow/2816467273/>>

<<http://www.flickr.com/photos/doctorow/2817314740/>>

Solitario:

<<http://www.schneier.com/solitaire.html>>

Le proposte:

<[http://www.boingboing.net/2008/09/05/help\\_design\\_a\\_cipher.html](http://www.boingboing.net/2008/09/05/help_design_a_cipher.html)>  
mailto:cryptocontest@craphound.com

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

Le news su Schneier/BT Counterpane

Schneier parlerà al World Economic Forum Annual Meeting of the New Champions, a Tianjin, in Cina, il 27 settembre.

<<http://www.weforum.org/en/events/AnnualMeetingoftheNewChampions2008/index.htm>>

oppure <<http://tinyurl.com/5ccexn>>

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

I controlli di documenti d'identità con foto negli aeroporti

La TSA sta inasprendo le regole riguardanti i documenti d'identità con foto nel contesto della sicurezza aeroportuale. In passato, le persone con documenti d'identità scaduti o che dichiaravano di averli perduti, venivano sottoposte a ulteriori controlli. Poi la Transportation Security Administration si è resa conto che se un individuo si trovava sulla no-fly list emanata dal governo (l'elenco che si dice dovrebbe tenere al sicuro i nostri aerei dai terroristi), poteva semplicemente volare senza documenti.

Ora, le persone prive di documenti di identità devono anche rispondere a domande personali sul proprio storico finanziario, in modo che sia possibile stabilirne l'identità. La TSA terrà dei registri per identificare queste persone senza documenti, nel caso si tratti di tentativi per saggiare la sicurezza del sistema.

Tutto questo, a prima vista, potrebbe sembrare un passo avanti -- solo che il requisito del documento con foto è un'idiozia. Chiunque si trovi sulla no-fly list può viaggiare con facilità ogni volta che vuole. Ancora peggio, l'intero concetto di confrontare nomi di passeggeri con un elenco di criminali ha un valore di sicurezza pressoché nullo.

Ecco il sistema per volare anche se ci si trova sulla no-fly list: comprate un biglietto aereo a nome di una persona innocente. A casa, prima di partire, effettuate il check-in online e stampate la vostra carta di imbarco. Poi salvate la pagina Web come file PDF e usate Adobe Acrobat per modificare il nome sulla carta di imbarco mettendoci il vostro. Stampate nuovamente il documento. All'aeroporto usate la carta d'imbarco fasulla e il vostro documento d'identità vero per passare i checkpoint di sicurezza. In fase di imbarco, usate la carta d'imbarco vera (ossia quella a nome di un altro) e salite a bordo.

Il problema è che a essere confrontati con la no-fly list sono nomi di passeggeri non verificati. Ai checkpoint di sicurezza, la TSA effettua semplicemente un confronto fra il documento di identità e il nome che viene stampato sulle carte d'imbarco. Quando i passeggeri si imbarcano, la compagnia aerea confronta le carte di imbarco con i

biglietti. Ma dato che nessuno mette a confronto i nomi sui biglietti con i documenti di identità, la sicurezza fallisce.

Questa vulnerabilità non è nuova. E non è nemmeno troppo oscura. Ne ho parlato nel 2003 e ancora nel 2006. Ho chiesto delucidazioni in merito al problema a Kip Hawley, il direttore della TSA, nel 2007. Oggi, qualsiasi terrorista abbastanza intelligente da cercare "come stamparsi una carta di imbarco" su Google, può aggirare la no-fly list.

Una tale falla di sicurezza mi darebbe ancor più fastidio se l'idea stessa di una no-fly list non fosse così inefficace. Il sistema è basato sulla concezione errata che i federali possiedono questo super-elenco permanente di nomi di terroristi, e tutto quel che occorre fare è allontanare dagli aerei le persone presenti in quell'elenco.

Ma non è affatto così. La no-fly list (un elenco di persone talmente pericolose che non hanno il permesso di volare, ma al tempo stesso così innocenti da non poter essere arrestate), e la meno pericolosa 'watch list' contengono insieme circa un milione di nominativi che rappresentano le identità e gli alias di circa 400.000 persone. Non vi sono così tanti terroristi là fuori; se ve ne fossero, ne sentiremmo gli effetti.

Quasi tutte le persone fermate dalla no-fly list sono dei falsi positivi. La lista ha colpito degli innocenti come Ted Kennedy, il cui nome è simile a quello di qualcuno nell'elenco, e Yusuf Islam (Cat Stevens), che si trovava nella lista ma nessuno sapeva perché.

La no-fly list è un incubo kafkiano per le migliaia di cittadini americani innocenti che vengono tormentati e arrestati ogni volta che viaggiano in aereo. Inseriti nella lista da funzionari del governo non identificati, non possono uscirne. Non possono contestare il loro status presso la TSA né provare la loro innocenza. (Questo mese, la U.S. 9th Circuit Court of Appeals ha stabilito che i passeggeri sulla no-fly list possono denunciare l'FBI, ma nessuno ha ancora provato tale strategia).

Ma anche se questi elenchi fossero completi e accurati, non funzionerebbero lo stesso. Timothy McVeigh, Unabomber, i cecchini di Washington DC, i dinamitardi della metropolitana londinese e la maggior parte dei terroristi dell'11 settembre non erano su nessuna 'lista nera' prima che commettessero i loro atti terroristici. E se un terrorista vuol sapere se si trova nell'elenco, la TSA ha approvato un servizio molto comodo, dal costo di 100 dollari, che gli permette di saperlo: il programma Clear, che emette dei documenti di identità a "viaggiatori fidati" per far sì che abbiano una corsia veloce ai checkpoint di sicurezza. Basta che facciate richiesta di una tessera Clear: se vi viene concessa, allora non siete sulla no-fly list.

Alla fin fine, il requisito del documento di identità con foto si basa sul mito per cui sia possibile, in qualche modo, correlare l'identità con l'intenzione. Non si può. E invece di buttare denaro facendo tentativi per dimostrarlo, saremmo tutti più sicuri come nazione se investissimo sull'intelligence, sull'investigazione e sulla risposta alle emergenze: misure di sicurezza che non si basano sull'indovinare quale sia il bersaglio o la tattica dei terroristi.

Questa è la TSA: un'entità che non fa le cose giuste. Che non fa nemmeno bene le cose che fa.

I miei precedenti articoli sul tema:

<<http://www.schneier.com/crypto-gram-0308.html#6>>

<[http://www.schneier.com/blog/archives/2006/11/forge\\_your\\_own.html](http://www.schneier.com/blog/archives/2006/11/forge_your_own.html)>  
<<http://www.schneier.com/interview-hawley.html>>

Questo articolo è originariamente apparso sul L.A. Times:  
<<http://www.latimes.com/news/opinion/la-oe-schneier28-2008aug28,0,3099808.story>>  
oppure <<http://tinyurl.com/6dmcl4>>

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

## Malattia mentale e omicidio

Contrariamente alla credenza popolare, gli omicidi dovuti a malattia mentale sono in recesso, almeno in Inghilterra e nel Galles: "Il tasso generale degli omicidi e il tasso di omicidi causati da disturbi mentali sono aumentati costantemente fino alla metà degli anni Settanta. Da quel momento vi è stata un'inversione nel tasso di omicidi dovuti a disturbi mentali, che è poi sceso a minimi storici, mentre altri tipi di omicidio hanno continuato ad aumentare".

Ricordatevelo la prossima volta che leggete un articolo su un giornale dove si parla dello spavento generale a seguito della fuga di alcuni pazienti da un ospedale psichiatrico: "Veniamo convinti dai mass media che gli individui con gravi malattie mentali abbiano una grossa parte negli omicidi, e in quanto società formuliamo il nostro approccio a decine di migliaia di persone sulla base delle azioni di circa 20 soggetti. Ancora una volta, le decisioni che prendiamo, gli atteggiamenti che abbiamo, e i pregiudizi che esprimiamo sono completamente razionali, se analizzati sulla base delle informazioni errate che ci arrivano, solo parzialmente masticate, dalle bocche dei cretini".

Gli articoli:

<<http://bjp.rcpsych.org/cgi/content/abstract/193/2/130>>  
<<http://www.badsience.net/2008/08/the-news-you-didnt-read/>>

Lo studio e il comunicato stampa:

<<http://www.scribd.com/doc/4805076/Homicide-due-to-mental-disorder-in-England-and-Wales-over-50-years>>  
oppure <<http://tinyurl.com/3w553h>>  
<<http://www.rcpsych.ac.uk/pressparliament/pressreleases2008/bank2008/prhomicide.aspx>>  
oppure <<http://tinyurl.com/3l3e3l>>

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

## Minacce da trama cinematografica

Spendiamo una gran quantità di denaro ed energie per difendere i nostri paesi contro specifiche minacce da trama cinematografica, piuttosto che contro le più grandi

minacce del terrorismo, che sono reali. Negli Stati Uniti, nei mesi successivi alla tragedia dell'11 settembre, avevamo paura di fantomatici gruppi di subacquei terroristi, di terroristi muniti di polverizzatori usati in agricoltura, di terroristi che contaminassero le nostre riserve di latte. Sia gli Stati Uniti che il Regno Unito hanno paura di terroristi muniti di bottigliette contenenti liquidi misteriosi. La nostra immaginazione si scatena elaborando minacce specifiche e ricche di dettagli. E in poco tempo iniziamo a tracciare un'intera trama da film, senza un Bruce Willis che salvi baracca e burattini. E abbiamo paura.

Non è solo il terrorismo, ma qualsiasi rischio raro che fa notizia. Adesso, a seguito di un incidente piuttosto raccapricciante, la grande paura in Canada, sono le possibili decapitazioni sugli autobus extraurbani. Negli Stati Uniti, la paura di un'altra sparatoria nelle scuole è molto più grande dei rischi effettivi. Nel Regno Unito, sono i predatori di bambini. E le persone in tutto il mondo hanno erroneamente più paura di volare che di andare in macchina. Ma la stessa definizione di 'news', di 'notizia', di 'novità', si riferisce a qualcosa che accade assai di rado. Se un incidente è fra le notizie, non dovremmo preoccuparci. È quando una cosa diventa così comune da non far più notizia (incidenti stradali, violenza domestica) che dovremmo preoccuparci. Ma questo non è il modo con cui la gente pensa.

Da un punto di vista psicologico, tutto questo è assolutamente legittimo. Siamo una razza di narratori. Abbiamo una buona immaginazione e rispondiamo più emotivamente alle storie che non ai dati. Inoltre giudichiamo la probabilità che qualcosa accada sulla base di quanto è facile immaginarla, pertanto le storie che fanno notizia sembrano più probabili, e inquietanti, delle storie che non arrivano a fare notizia. Di conseguenza abbiamo una reazione esagerata nei confronti di rischi rari di cui sentiamo parlare, e abbiamo paura di complotti specifici più che di minacce generalizzate.

Il problema della sicurezza che viene creata intorno a specifici bersagli e a determinate tattiche è che funziona soltanto se indoviniamo correttamente il complotto. Se spendiamo miliardi di dollari per difendere la rete metropolitana e i terroristi fanno saltare in aria una scuola, quelli sono soldi sprecati. Se ci concentriamo sui Mondiali di calcio e i terroristi attaccano Wimbledon, anche in questo caso avremo investito denaro inutilmente.

È questa attenzione feticistica sulle tattiche che genera le follie di sicurezza negli aeroporti. Vietiamo pistole e coltelli, e i terroristi usano dei taglierini. Vietiamo taglierini e cavatappi, e nascondono gli esplosivi nelle scarpe. Controlliamo le scarpe, e i terroristi utilizzano i liquidi. Vietiamo i liquidi, e i terroristi si serviranno di qualcos'altro. Oppure ignoreranno del tutto gli aerei e attaccheranno una scuola, una chiesa, un teatro, uno stadio, un centro commerciale, il terminal di un aeroporto fuori dall'area di sicurezza, o un qualsiasi luogo intensamente affollato.

Sono giochetti stupidi, questi, e allora smettiamola di giocare. Esistono bersagli di alto profilo che meritano un'attenzione particolare, e certe tattiche sono peggiori di altre. Gli aerei sono un bersaglio particolarmente importante, perché sono simboli nazionali e perché un ordigno di ridotte dimensioni può provocare la morte di tutti gli occupanti. Anche le sedi governative sono bersagli simbolici e quindi interessanti. Ma bersagli e tattiche sono intercambiabili.

Dobbiamo difenderci contro la minaccia del terrorismo in generale, non contro particolari minacce da trama cinematografica. La sicurezza è al massimo dell'efficienza

quando non ci richiede di fare supposizioni arbitrarie. Occorre investire più risorse nell'intelligence e nell'investigazione: identificare i terroristi stessi, impedire che vengano finanziati, e fermarli a prescindere dalle loro intenzioni. Occorre investire più risorse nella risposta alle emergenze: ridurre al massimo l'impatto di un attacco terroristico, non importa quale esso sia e come avvenga. E dobbiamo affrontare le conseguenze geopolitiche della nostra politica estera.

Nel 2006, la polizia britannica ha arrestato i dinamitardi degli esplosivi liquidi non grazie a una assidua sicurezza aeroportuale, ma servendosi di intelligence e di investigazioni. Quale fosse il bersaglio dei dinamitardi, quali fossero le loro tattiche, non aveva importanza. Sarebbero stati arrestati comunque. Questa è sicurezza intelligente. Ora confisciamo i liquidi negli aeroporti, in caso qualche altro gruppo terroristico possa attaccare lo stesso identico bersaglio nello stesso identico modo. È semplicemente illogico.

Questo articolo è originariamente apparso nel Guardian. Niente che non abbia già detto in altre circostanze.

<<http://www.guardian.co.uk/technology/2008/sep/04/terrorism.terrorismandtravel>>

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

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

Commenti dei lettori

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

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

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

CRYPTO-GRAM è una newsletter mensile gratuita che offre riassunti, analisi, approfondimenti, e commenti sulla sicurezza (informatica e in generale) e sulla crittografia. I numeri arretrati sono disponibili all'indirizzo

<<http://www.schneier.com/crypto-gram.html>>. Per iscriversi, cancellare l'iscrizione o

cambiare il proprio indirizzo a cui recapitare la newsletter, visitate sempre

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

La versione italiana è curata da Communication Valley SpA

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

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

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

Per informazioni <crypto-gram@communicationvalley.it>

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

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

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

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

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

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

Copyright (c) 2008 - Bruce Schneier.