

CRYPTO-GRAM  
15 settembre 2005

Scritta da Bruce Schneier  
Fondatore e CTO di Counterpane Internet Security, Inc.

Edizione italiana curata da Communication Valley SpA

E-mail: [schneier@counterpane.com](mailto:schneier@counterpane.com)

Web: [<http://www.schneier.com>](http://www.schneier.com) oppure [<http://www.counterpane.com>](http://www.counterpane.com)

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

Crypto-Gram in versione originale è anche consultabile in formato RSS:  
[<http://www.schneier.com/crypto-gram-rss.xml>](http://www.schneier.com/crypto-gram-rss.xml)

Gli stessi articoli della newsletter sono disponibili sul blog di Bruce Schneier:  
[<http://www.schneier.com/blog>](http://www.schneier.com/blog).

\*\* \*\*

In questo numero:

Le minacce da trama cinematografica  
L'uragano Katrina e la sicurezza  
Le chiavi della metropolitana di Sydney  
Le ristampe di Crypto-Gram  
Nuovi risultati crittanalitici contro SHA-1  
Zotob  
News  
Sicurezza aerea, compromessi e agenda  
Telecamere di sorveglianza nella metropolitana di New York  
Le News di Counterpane  
Lance Armstrong accusato di doping  
Peggy Noonan e le minacce terroristiche da trama cinematografica  
Le buone pratiche del Trusted Computing  
Commenti dei lettori

\*\* \*\*

Le minacce da trama cinematografica

A volte sembra proprio che chi è incaricato della sicurezza nazionale passi troppo tempo a guardare film d'azione e che quindi organizzi una difesa contro specifiche minacce da trama cinematografica, piuttosto che contro le più vaste minacce del terrorismo.

Capita a tutti: la nostra immaginazione si scatena elaborando minacce specifiche e ricche di dettagli. Ci immaginiamo che dai polverizzatori usati in agricoltura si propaghi antrace. O pensiamo a una fornitura di latte contaminata. O a gruppi di subacquei terroristi armati di calendari. Poco dopo iniziamo a tracciare un'intera trama da film, senza un Bruce Willis che salvi baracca e burattini. E abbiamo paura.

Da un punto di vista psicologico, tutto questo è assolutamente legittimo. Gli esseri umani sono dotati di una forte immaginazione. Taglierini ed esplosivi nascosti in scarpe evocano immagini mentali assai vivide. “Dobbiamo proteggere il SuperBowl” ha un impatto emotivo molto più intenso che non un vago “dobbiamo difenderci dal terrorismo”.

I terroristi dell'11 settembre hanno utilizzato piccoli oggetti appuntiti per dirottare gli aerei, allora noi vietiamo l'introduzione di piccoli oggetti appuntiti sugli aerei. Richard Reid ha provato a nascondere una bomba all'interno delle sue scarpe, quindi ora dobbiamo tutti toglierci le scarpe al checkpoint. Recentemente il Dipartimento per la Sicurezza Nazionale ha dichiarato che potrebbe allentare le restrizioni di sicurezza che riguardano l'imbarco sugli aerei. Ma non perché vi sia un minor rischio di trovare bombe all'interno di scarpe, o perché all'improvviso i piccoli oggetti appuntiti di cui sopra siano diventati meno pericolosi. La ragione è che quelle contromisure da trama cinematografica non catturano più l'immaginario collettivo come succedeva nei mesi successivi alla tragedia dell'11 settembre, e tutti stanno cominciando a rendersi conto di quanto siano state sciocche e immotivate.

Adesso la nuova trama da film d'azione riguarda il terrorismo ai danni dei pendolari. I dinamitardi di Londra hanno portato ordigni esplosivi all'interno della metropolitana, quindi ora perquisiamo le persone che entrano nelle stazioni della metropolitana. Si sono serviti di telefoni cellulari, e allora adesso si fa un gran discutere su come disattivare la rete cellulare.

È troppo presto per poter dire con sicurezza che la prossima minaccia da trama cinematografica saranno gli uragani...

Il problema di tutta questa sicurezza “da film” è che funziona soltanto se ci azzecchiamo. Se spendiamo miliardi di dollari per difendere le metropolitane, e poi i terroristi piazzano un ordigno su un autobus, abbiamo buttato i nostri soldi. Certo, difendere le metropolitane rende più sicuro il pendolarismo. Ma concentrarsi unicamente sulle metropolitane ha anche l'effetto di spostare gli attacchi verso bersagli meno difesi, e il risultato è che in generale siamo tutti meno sicuri.

Ai terroristi non importa far saltare metropolitane, autobus, stadi, teatri, ristoranti, night-club, scuole, chiese, mercati affollati o svincoli autostradali durante le ore di punta. È ragionevole affermare come alcuni bersagli siano innegabilmente più allettanti di altri: gli

aerei, perché un ordigno di ridotte dimensioni può provocare la morte di tutti gli occupanti; i monumenti, per il loro significato a livello nazionale; eventi nazionali, per la presenza della televisione e dei media; i trasporti, perché la maggioranza dei lavoratori li utilizza quotidianamente. Ma gli Stati Uniti sono un paese enorme: non possiamo difendere qualsiasi cosa.

Un problema è dato dal fatto che i leader del nostro paese ci stanno dando quel che vogliamo. A prescindere dall'orientamento politico, è importante apparire molto duri nei confronti del terrorismo. Votare in favore di una difesa missilistica procura una campagna elettorale migliore che non l'aumentare i finanziamenti per l'intelligence. Chi viene eletto vuole fare qualcosa di visibile, anche se si rivela totalmente inefficace.

L'altro problema è che molte decisioni di sicurezza vengono prese a un livello troppo basso. La decisione di spegnere i cellulari in alcuni passaggi sotterranei è stata presa da chi aveva la responsabilità di quei tunnel. Anche se i terroristi bombardassero un tunnel diverso in un'altra parte del paese, quelle persone avrebbero svolto il loro lavoro.

E chiunque sia incaricato della sicurezza sa che verrà giudicato col senno di poi. Se il prossimo attacco terroristico ha come bersaglio una centrale nucleare, noi esigeremo sapere perché non si è fatto di più per proteggere le centrali nucleari. Se la minaccia colpirà gli alunni di una scuola elementare, esigeremo sapere perché tale minaccia è stata ignorata. Non accetteremo un "non sapevamo quale sarebbe stato il bersaglio" come risposta. Difendere alcuni bersagli specifici protegge reputazioni e carriere.

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 fa supposizioni arbitrarie in merito al prossimo atto terroristico. Occorre investire più denaro nell'intelligence e in indagini: identificare i terroristi stessi, impedire che vengano finanziati, e fermarli a prescindere dalle loro intenzioni. Occorre investire più denaro nella risposta alle emergenze: ridurre al massimo l'impatto di un attacco terroristico, non importa quale esso sia e come avvenga. Dobbiamo affrontare le conseguenze geopolitiche della nostra politica estera e come essa favorisca o impedisca il terrorismo.

Queste vaghe risoluzioni sono meno visibili, e non aiutano a mettersi in mostra politicamente. Ma ci renderanno più sicuri. Sprecare denaro per la minaccia da trama cinematografica dell'anno, no di certo.

Questo articolo è stato originariamente pubblicato su Wired:  
<<http://www.wired.com/news/business/0,1367,68789,00.html>>

Per Wired sto inoltre scrivendo un articolo d'opinione a cadenza bisettimanale. Potete leggere i miei interventi su Wired.com, o potete aspettare che li ripubblichi su Crypto-Gram.

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

## L'uragano Katrina e la sicurezza

Lasciando da parte per un momento gli atteggiamenti politici e le dita puntate, come hanno fatto gli Stati Uniti a gestire così malamente la situazione Katrina? Dopo aver speso decine di miliardi di dollari in sicurezza nazionale (centinaia di miliardi, se contiamo anche il conflitto in Iraq) nei quattro anni che hanno seguito la tragedia dell'11 settembre, che cosa abbiamo sbagliato? Perché vi sono stati così tanti errori ed omissioni a livello locale, statale e federale?

Sono domande che è lecito porsi. Katrina è stato un disastro naturale e non un attacco terroristico, ma questo importa soltanto prima dell'evento. Gli attacchi terroristici su vasta scala e i disastri naturali differiscono solo nelle cause, ma hanno effetti e conseguenze molto simili. Non è difficile immaginare che un attacco terroristico porti a conseguenze simili al disastro provocato da un uragano, specialmente un atto terroristico che preveda l'uso di armi nucleari, biologiche o chimiche.

Migliorare la nostra risposta alle calamità è stato uno degli argomenti di discussione nei mesi che seguirono l'11 settembre. Avremmo dato il nostro denaro ai governi locali per finanziare i "first responder", i primi a rispondere alle emergenze. Abbiamo incaricato il Dipartimento per la Sicurezza Nazionale di semplificare le gerarchie di comando e di facilitare una risposta efficiente ed efficace.

Il problema è che ci siamo tutti fatti intrappolare dalle "minacce da trama cinematografica", ovvero specifici scenari d'attacco che attraggono prima l'immaginazione e poi il denaro. Che si tratti di terroristi muniti di taglierini o di esplosivi nelle scarpe, abbiamo paura di ciò che ci è dato immaginare. Ci mettiamo a perquisire gli zaini nella metropolitana di New York, perché la "minaccia da film" in voga quest'anno è basata su un terrorista che piazza bombe nelle stazioni della metropolitana di Londra.

Finanziare una sicurezza basata su trame cinematografiche fa una gran figura in televisione, e porta certa gente ad essere rieledda. Ma scenari possibili ve ne sono a milioni, e non è facile indovinare. I miliardi spesi per difendere le linee aeree sono denaro sprecato se poi i terroristi fanno saltare centri commerciali affollati.

Gli Stati Uniti devono spendere i dollari per la sicurezza nazionale in due cose: intelligence e risposta alle emergenze. Queste due cose

daranno un grande contributo a prescindere da ciò che stanno preparando i terroristi, e la seconda è d'aiuto sia contro il terrorismo sia in caso di calamità naturali.

Katrina ha dimostrato che non è stato investito sufficiente denaro nella risposta alle emergenze. Gli agenti di polizia di New Orleans non erano in grado di comunicare fra di loro dopo che i black-out hanno chiuso il loro sistema di comunicazione principale -- e non c'erano rinforzi. Il Dipartimento per la Sicurezza Nazionale, che era stato costituito per centralizzare la risposta federale in una situazione come questa, non è stato in grado di capire chi dirigesse le operazioni e che cosa fare, e ha seriamente ostacolato l'aiuto di terzi. La FEMA non ha fatto meglio, e sono morte migliaia di persone mentre si combattevano guerre tra fazioni.

L'inettitudine del governo statunitense nella situazione post-uragano dimostra quanto poco otteniamo da tutto quel che si è dilapidato in sicurezza. È inconcepibile che si stia sprecando denaro prendendo le impronte digitali agli stranieri, effettuando il profiling dei passeggeri delle linee aeree, e invadendo altri paesi mentre la risposta nazionale alle emergenze non viene sufficientemente finanziata.

I dollari investiti nella risposta alle emergenze ci rendono più sicuri, a prescindere da quale sarà il prossimo disastro, naturale o terroristico.

Questo comprende un'ottima comunicazione a valle, un ottimo coordinamento a monte, e risorse (persone e rifornimenti) che possano venire movimentate con rapidità dovunque siano necessarie.

Analogamente, il denaro investito nella raccolta di intelligence ci rende più sicuri, a prescindere da quale sarà il prossimo disastro. Contro il terrorismo, coinvolgendo NSA e CIA; contro le calamità naturali, coinvolgendo il National Weather Service (servizio meteo nazionale) e il National Earthquake Information Center (centro nazionale di informazioni sismiche).

Katrina ha ampiamente illustrato la sfida più grande per la sicurezza nazionale: indovinare correttamente. La soluzione è finanziare un tipo di sicurezza che non si affida alle congetture. Difendersi contro minacce da trama cinematografica non ci rende apprezzabilmente più sicuri. La risposta alle emergenze sì. Riduce i danni e le sofferenze causate dai disastri, che siano per mano dell'uomo (come l'11 settembre) o della natura, come l'uragano Katrina.

Questo articolo è stato originariamente pubblicato sul Minneapolis Star Tribune:

<http://www.startribune.com/stories/562/5606306.html>

Qui potete trovare le mie riflessioni preliminari:

[http://www.schneier.com/blog/archives/2005/09/security\\_lesson.html](http://www.schneier.com/blog/archives/2005/09/security_lesson.html)

\*\* \*\*

Le chiavi della metropolitana di Sydney

In genere, i segreti globali sono considerati scarsa sicurezza. Il problema è duplice. In primo luogo, non è possibile applicare alcuna gradualità al sistema di sicurezza: o uno conosce il segreto o non lo conosce. Secondariamente, i segreti globali sono fragili, e falliscono drammaticamente: se il segreto viene divulgato, allora gli aggressori si ritrovano con un segreto piuttosto potente.

Questa è la situazione attuale a Sydney, dove qualcuno ha rubato il passe-partout che consente l'accesso a qualsiasi treno dell'area metropolitana e l'avvio del treno stesso.

Purtroppo non si tratta di un ladruncolo che ha avuto un colpo di fortuna. Questo fatto è accaduto due volte a Sydney, ed è possibile che il bersaglio fosse proprio quella chiave.

E dunque, che può fare qualcuno in possesso del passe-partout della metropolitana di Sydney? Più probabilmente si tratta di un criminale, non di un terrorista, ma anche in questo caso il problema non è meno grave.

Non so se RailCorp debba sostituire le serrature. Non sono a conoscenza dei rischi: non so se quel "range di misure di sicurezza" protegga solo contro il furto di treni (uno scenario improbabile, se volete una mia opinione) o anche contro altri potenziali scenari. E non so quanto possa costare la sostituzione di tutte le serrature.

Un altro problema dei segreti globali è che ripristinare la situazione dopo una falla di sicurezza, solitamente, è piuttosto costoso.

Questa di sicuro non è la prima volta che un passe-partout è finito in mani sbagliate: "[Il direttore capo di RailCorp] Vince Graham ha dichiarato che non aveva senso cambiare alcuna delle serrature della linea metropolitana.

“Potremmo cambiare le serrature una volta alla settimana, ma non credo che questo riduca di molto la minaccia di sicurezza, dato che vi sono 2.000 di queste chiavi speciali rilasciate allo staff operativo lungo tutta la rete, e ritengo che costituirà sempre un problema”.

Un ultimo problema dei segreti globali è che è sempre molto facile perderne il controllo.

Morale: non affidatevi a segreti globali.

[http://www.schneier.com/blog/archives/2005/09/the\\_keys\\_to\\_the.html](http://www.schneier.com/blog/archives/2005/09/the_keys_to_the.html)  
<http://smh.com.au/news/national/two-sets-of-keys-to-sydneys-trains-stolen/2005/08/30/1125302547374.html> oppure <http://tinyurl.com/bpk4a>  
<http://news.ninemsn.com.au/article.aspx?id=15096>

\*\* \*\*

Le ristampe di Crypto-Gram

Crypto-Gram è attualmente al suo ottavo anno di pubblicazione. I numeri precedenti coprono tutta una serie di argomenti legati alla sicurezza e si possono trovare a questo indirizzo:

<http://www.schneier.com/crypto-gram.html>. Quella che segue è una selezione di articoli apparsi in questo mese gli anni scorsi.

La sicurezza alle Olimpiadi:

<http://www.schneier.com/crypto-gram-0409.html#2>  
<http://www.cryptogram.it/cryptogramPdf/Settembre2004.pdf> (versione italiana)

Il programma Trusted Traveler:

<http://www.schneier.com/crypto-gram-0409.html#5>  
<http://www.cryptogram.it/cryptogramPdf/Settembre2004.pdf> (versione italiana)

La cosiddetta "No-Fly List":

<http://www.schneier.com/crypto-gram-0409.html#10>  
<http://www.cryptogram.it/cryptogramPdf/Settembre2004.pdf> (versione italiana)

Incidenti fortuiti e incidenti di sicurezza:

<http://www.schneier.com/crypto-gram-0309.html#1>  
<http://www.cryptogram.it/settembre03.htm#a1> (versione italiana)

Worm benigni:

<http://www.schneier.com/crypto-gram-0309.html#8>  
<http://www.cryptogram.it/settembre03.htm#a8> (versione italiana)

Numero speciale sull'11 settembre, comprendente articoli sulla sicurezza negli aeroporti, sulla biometrica, sulla crittografia, la steganografia, gli insuccessi dell'intelligence, e sulla protezione della libertà:

<http://www.schneier.com/crypto-gram-0109a.html>

L'Esposizione Totale e la Finestra di Esposizione:

<http://www.schneier.com/crypto-gram-0009.html#1>

Open Source e sicurezza:



<[http://www.educatedguesswork.org/movabletype/archives/2005/07/deploying\\_a\\_new.html](http://www.educatedguesswork.org/movabletype/archives/2005/07/deploying_a_new.html)> oppure <<http://tinyurl.com/cz4lf>>

I due studi di Xiaoyun Wang, da Crypto:

Efficient Collision Search Attacks on SHA-0 [Attacchi collision search efficaci contro SHA-0]:

<<http://202.194.5.130/admin/infosec/download.php?id=1>>

Finding Collisions in the Full SHA-1 [La ricerca di collisioni nell'algorithmo SHA-1 completo]:

<<http://202.194.5.130/admin/infosec/download.php?id=2>>

Gli altri suoi studi:

<<http://www.infosec.sdu.edu.cn/people/wangxiaoyun.htm>>

La vicenda dei visti d'ingresso USA negati per partecipare alla conferenza:

<[http://www.schneier.com/blog/archives/2005/08/chinese\\_cryptog.html](http://www.schneier.com/blog/archives/2005/08/chinese_cryptog.html)>

<<http://www.navyseals.com/community/articles/article.cfm?id=7757>>

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

Zotob

Ho avuto modo di leggere l'imponente copertura stampa su Zotob, e non riesco a capire quale sia la gran notizia. Sì, si propaga in Windows 2000 senza l'intervento dell'utente, che è sempre una brutta cosa. Sfrutta una vulnerabilità del plug-and-play di Microsoft, che è un elemento piuttosto interessante. Ma l'unico motivo che posso immaginare del perché la CNN ne ha parlato così tanto è che la CNN stessa è stata colpita da Zotob.

<[http://www.theregister.co.uk/2005/08/15/zytob\\_worm/print.html](http://www.theregister.co.uk/2005/08/15/zytob_worm/print.html)>

<<http://www.securityfocus.com/news/11281>>

<<http://news.ft.com/cms/s/112bcc04-0f0d-11da-8b31-00000e2511c8.html>>

<[http://www.theregister.co.uk/2005/08/16/irc\\_bot/](http://www.theregister.co.uk/2005/08/16/irc_bot/)>

<<http://it.slashdot.org/it/05/08/16/2247228.shtml?tid=220&tid=188>>

<<http://www.computerworld.com/printthis/2005/0,4814,103929,00.html>>

<[http://www.newsfactor.com/story.xhtml?story\\_id=37727](http://www.newsfactor.com/story.xhtml?story_id=37727)>

<<http://www.pcworld.idg.com.au/index.php/id;1841567960;fp;2;fpid;1>>

<<http://www.securityfocus.com/news/11285>>

Dettagli tecnici:

<<http://www.sophos.com/virusinfo/analyses/w32zotoba.html>>

<[http://www.f-secure.com/v-descs/zotob\\_a.shtml](http://www.f-secure.com/v-descs/zotob_a.shtml)>

<<http://securityresponse.symantec.com/avcenter/venc/data/w32.zotob.a.htm>

>

oppure <<http://tinyurl.com/8so5h>>

Vulnerabilità:

<<http://www.microsoft.com/technet/security/Bulletin/MS05-039.msp>>

\*\* \*\*

## News

SANS NewsBites è una raccolta settimanale delle storie di sicurezza informatica che accadono là fuori. Ci sono commenti, ma sono ridotti al minimo. Si tratta in primis di brevi descrizioni e di link ad articoli di informazione. Vi sono parecchie newsletter leggibili via e-mail, ma leggo sempre questa. L'iscrizione è gratuita, il che è un'ottima cosa, dato che si tratta di una delle risorse di informazione sulla sicurezza informatica più utili in tutta Internet. Fra parentesi, faccio parte del comitato editoriale. Per iscriversi e per i numeri arretrati:

<http://www.sans.org/newsletters>

Ricerca sull'analisi del rischio comportamentale:

<https://www.fastlane.nsf.gov/servlet/showaward?award=0527598>

Interessante articolo di giurisprudenza sulle fonti di informazione che facilitano il compimento di un reato:

<http://www.law.ucla.edu/volokh/facilitating.pdf>

Uno schermo con funzioni di salvaguardia della privacy:

<http://www.merl.com/projects/privatedisplay/>

Se si possiede una registrazione audio di qualcuno che batte su una normale tastiera di un computer per circa quindici minuti, è possibile ricostruire tutto quello che ha scritto.

<http://www.freedom-to-tinker.com/?p=893>

[http://www.cs.berkeley.edu/~tygar/papers/Keyboard\\_Acoustic\\_Emanations\\_Revisited/preprint.pdf](http://www.cs.berkeley.edu/~tygar/papers/Keyboard_Acoustic_Emanations_Revisited/preprint.pdf) oppure <http://tinyurl.com/dzgda>

Mettendo da parte per un momento le questioni geopolitiche, è interessante leggere i dettagli tecnici di sicurezza della barriera costruita dagli israeliani intorno a Gaza:

<http://www.jpost.com/servlet/Satellite?pagename=JPost/JPArticle/ShowFull&cid=1126059637154> oppure <http://tinyurl.com/bsjyb>

In "Beyond Fear", pagg. 207-8, ho parlato dei dettagli tecnici del muro di Berlino. Qui il tutto è molto più sofisticato.

"Le sei idee più stupide in materia di sicurezza informatica" di Marcus Ranum:

[http://www.ranum.com/security/computer\\_security/editorials/dumb/](http://www.ranum.com/security/computer_security/editorials/dumb/)

I criminali stanno imparando la scienza forense, e le giurie si stanno creando aspettative irrealistiche sulla scienza forense, in entrambi i casi grazie a show televisivi come CSI.

<http://www.newscientist.com/channel/opinion/mg18725163.800>

Un affascinante articolo su A.G. Tolkachev, una spia russa che ha lavorato per la CIA per una decina d'anni. Mi ha interessato in particolare modo leggere le descrizioni sull'abilità di negoziare.

<http://www.cia.gov/csi/studies/vol47no3/article02.html>

Un orribile articolo che suggerisce l'implementazione di un firewall nazionale USA:

<http://www.pcmag.com/article2/0,1895,1831969,00.asp>

Un criminale ha videoregistrato delle chiavi mentre venivano utilizzate, in modo da poterle in seguito duplicare:

<http://www.philly.com/mlp/philly/news/local/12554094.htm?template=contentModules/printstory.jsp> oppure <http://tinyurl.com/7pd2n>

Un ricercatore parla di come i criminali si adattino alle funzionalità di sicurezza delle carte di identità, come il chip and PIN:

[http://www.schneier.com/blog/archives/2005/09/identity\\_cards.html](http://www.schneier.com/blog/archives/2005/09/identity_cards.html)

<http://www.guardian.co.uk/crime/article/0,2763,1562681,00.html>

<http://smh.com.au/news/World/New-tech-may-increase-ID-theft-expert/2005/09/05/1125772436375.html> oppure <http://tinyurl.com/7759a>

<http://news.bbc.co.uk/1/hi/sci/tech/4213848.stm>

<http://software.silicon.com/security/0,39024655,39151961,00.htm>

La mailing list Digital-ER è dedicata alla discussione di soluzioni tecniche per la gestione delle emergenze e delle crisi.

<http://lists.networkcommand.com/mailman/listinfo/digital-er>

Una storia divertente, e tragica in ultima analisi, su un poco efficiente generatore di numeri casuali usato in un gioco televisivo.

[http://www.rotten.com/library/conspiracy/Press\\_Your\\_Luck/](http://www.rotten.com/library/conspiracy/Press_Your_Luck/)

Sicurezza a Hogwarths:

[http://www.schneier.com/blog/archives/2005/09/hogwarts\\_security.html](http://www.schneier.com/blog/archives/2005/09/hogwarts_security.html)

<http://ritestuff.blogspot.com/2005/08/harry-potter-and-half-assed-security.html> oppure <http://tinyurl.com/9smud>

<http://www.veryard.com/trust/potter.htm>

Su SlashDot c'è una discussione riguardante la sicurezza del code signing, e in particolare modo sui miei commenti in materia nel libro "Secrets and Lies".

<http://ask.slashdot.org/askslashdot/05/08/31/2045201.shtml?tid=172&tid=156&tid=4> oppure <http://tinyurl.com/bsbd7>

Cryptome ha un elenco di 276 agenti MI6:

<http://cryptome.org/mi6-list-276.htm>

Si discuta la sicurezza, la legalità, l'etica e il buon senso di tutto ciò a questo indirizzo:

[http://www.schneier.com/blog/archives/2005/08/276\\_british\\_spi.html](http://www.schneier.com/blog/archives/2005/08/276_british_spi.html)

Ecco un nuovo programma di ricerca sulla raccolta dati via Internet con un bel nome: Unintended Information Revelation [Rivelazione involontaria

di informazioni].

<http://www.contractoruk.com/news/002194.html>

La sicurezza delle buste cosiddette “tamper-evident” (cioè che non è possibile aprirle senza danneggiarle), del genere usato dalle banche e dalle compagnie di carte di credito per inviare codici PIN e password:

<http://www.schneier.com/blog/archives/2005/08/tamper-evident.html>

<http://news.bbc.co.uk/1/hi/technology/4183330.stm>

<http://www.cl.cam.ac.uk/~mkb23/research/PIN-Mailer.pdf>

Buon articolo sulla sicurezza di Visa, alla luce dell'incidente di CardSystems.

<http://www.nytimes.com/2005/08/25/business/25visa.html>

L'articolo riprende alcune argomentazioni sulla sicurezza che ho trattato qui:

[http://www.schneier.com/blog/archives/2005/07/visa\\_and\\_amex\\_d.html](http://www.schneier.com/blog/archives/2005/07/visa_and_amex_d.html)

Un ladro di identità ruba una casa:

<http://www.plastic.com/article.html;sid=05/08/23/19205287;cmt=60>

Un impiegato della Cingular ha venduto telefoni cellulari usati ancora contenenti le informazioni dei proprietari:

[http://www.schneier.com/blog/archives/2005/08/privacy\\_risks\\_o.html](http://www.schneier.com/blog/archives/2005/08/privacy_risks_o.html)

[http://www.wfmynews2.com/watercooler/watercooler\\_article.aspx?storyid=47473](http://www.wfmynews2.com/watercooler/watercooler_article.aspx?storyid=47473) oppure <http://tinyurl.com/dggys>

I rischi legati alla perdita di dispositivi portatili:

[http://www.schneier.com/blog/archives/2005/07/risks\\_of\\_losing.html](http://www.schneier.com/blog/archives/2005/07/risks_of_losing.html)

I computer del governo statunitense attaccati dalla Cina:

<http://www.washingtonpost.com/wp-dyn/content/article/2005/08/24/AR2005082402318.html>

oppure <http://tinyurl.com/bup8w>

Lo sapevate che potreste essere arrestati a New York se siete in possesso di un'uniforme di polizia? Persino se siete un attore che sta recitando la parte di un poliziotto in un film o spettacolo?

[http://www.schneier.com/blog/archives/2005/08/actors\\_playing.html](http://www.schneier.com/blog/archives/2005/08/actors_playing.html)

[http://www.usatoday.com/life/television/news/2005-08-22-sag-warning\\_x.htm](http://www.usatoday.com/life/television/news/2005-08-22-sag-warning_x.htm) oppure <http://tinyurl.com/a8f5w>

Interessante borsa di ricerca da parte della NSF: un approccio socio-tecnico alla sicurezza informatica.

<https://www.fastlane.nsf.gov/servlet/showaward?award=0550008>

Ecco una parte di una ricerca molto interessante portata avanti dallo stato dell'Ohio: si tratta di un sensore passivo che potrebbe risultare più economico, migliore, e meno invadente di tecnologie come i raggi X a retrodiffusione.

[http://www.schneier.com/blog/archives/2005/08/ambient\\_radiati.html](http://www.schneier.com/blog/archives/2005/08/ambient_radiati.html)

<http://www.sciencedaily.com/releases/2005/08/050814172841.htm>

Degli inserzionisti inviano pubblicità indesiderata ai telefonini Bluetooth alla distanza di 100 metri.

[http://www.schneier.com/blog/archives/2005/08/bluetooth\\_spam.html](http://www.schneier.com/blog/archives/2005/08/bluetooth_spam.html)

<http://www.newscientist.com/article.ns?id=dn7883>

RFID nelle targhe automobilistiche britanniche:

<http://www.wired.com/news/privacy/0,1848,68429,00.html>

Dei ladri stanno utilizzando dei cellulari Bluetooth per trovare computer portatili con porta Bluetooth lasciati in auto parcheggiate, per poi rubarli.

[http://www.cambridge-news.co.uk/news/region\\_wide/2005/08/17/06967453-8002-45f8-b520-66b9bed6f29f.lpf](http://www.cambridge-news.co.uk/news/region_wide/2005/08/17/06967453-8002-45f8-b520-66b9bed6f29f.lpf) oppure <http://tinyurl.com/ey9zw>

Buon esempio di conseguenze di sicurezza impreviste di una nuova tecnologia e prova ulteriore che le nuove funzionalità devono essere disattivate per default.

Neonati sulla watch list antiterrorismo:

[http://www.schneier.com/blog/archives/2005/08/infants\\_on\\_the.html](http://www.schneier.com/blog/archives/2005/08/infants_on_the.html)

<http://www.cnn.com/2005/TRAVEL/08/15/no.fly.babies.ap/index.html>

“I 13 di Kutztown”: tredici ragazzi della scuola superiore sono stati accusati di gravi reati per aver aggirato la sicurezza dei computer portatili forniti dalla scuola.

[http://www.schneier.com/blog/archives/2005/08/computer\\_crime.html](http://www.schneier.com/blog/archives/2005/08/computer_crime.html)

[http://www.theregister.co.uk/2005/08/10/kutztown\\_13/](http://www.theregister.co.uk/2005/08/10/kutztown_13/)

<http://www.wired.com/news/technology/0,1282,68480,00.html>

[http://www.usatoday.com/tech/columnist/andrewkantor/2005-08-18-kutztown-kids\\_x.htm](http://www.usatoday.com/tech/columnist/andrewkantor/2005-08-18-kutztown-kids_x.htm) oppure <http://tinyurl.com/9a8ql>

Le accuse sono state poi ritirate:

<http://it.slashdot.org/article.pl?sid=05/09/02/0712237>

Pare che il Dipartimento per la Sicurezza Nazionale e la TSA stiano finalmente iniziando a capire che piccoli oggetti appuntiti non sono una minaccia terroristica per l'aviazione.

<http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2005/08/13/national/w234140D88.DTL>

oppure <http://tinyurl.com/d6wr4>

Le conseguenze sulla privacy della presenza di aerei senza equipaggio che pattugliano le frontiere:

<http://www.epic.org/privacy/surveillance/spotlight/0805/>

\*\* \*\*

Sicurezza aerea, compromessi e agenda

Tutte le decisioni di sicurezza sono compromessi, bilanciamenti, e i compromessi di sicurezza più intelligenti sono quelli dove la sicurezza

ottenuta vale pienamente ciò a cui si è rinunciato per ottenerla. Tutto questo suona facile, ma non lo è. Vi sono delle belle differenze fra rischio percepito e rischio effettivo, differenze fra sicurezza percepita e sicurezza effettiva, e differenze fra costi percepiti e costi effettivi. Oltre a questo, vi sono legittime differenze nell'analisi dei compromessi. Una qualsiasi complicata decisione di sicurezza influenza molteplici attori, ed ognuno di essi valuta il compromesso dal proprio punto di vista.

Io definisco tutto ciò "agenda", ed è uno dei temi centrali di "Beyond Fear". È illustrato con chiarezza nell'attuale discussione sull'eliminazione del divieto di portare piccoli oggetti appuntiti sugli aerei. Gli assistenti di volo sono contro tale cambiamento. Leggendo i loro commenti, potete chiaramente vedere quale sia la loro agenda soggettiva:

“Come il personale in prima linea senza un addestramento di sicurezza efficace o mezzi di autodifesa, tali oggetti potrebbero rivelarsi fatali per i nostri membri”, ha dichiarato Patricia A. Friend, presidente internazionale dell'Associazione degli Assistenti di Volo (Association of Flight Attendants), in una lettera a Edmund S. 'Kip' Hawley, il nuovo capo della TSA. 'Potrebbero non servire a forzare il portello della cabina di pilotaggio, ma potrebbero sicuramente provocare la morte di assistenti di volo e passeggeri'...

“Gli assistenti di volo, la cui unione rappresenta 46.000 membri, hanno dichiarato che eliminare il divieto su alcuni oggetti proibiti potrebbe comportare un rischio di sicurezza a bordo dell'aereo e provocare incidenti che inducono panico nei passeggeri anche se non si tratta di un dirottamento.

“Anche nel caso in cui un aereo venisse attaccato e l'incidente si limitasse soltanto ad alcune morti, questo potrebbe seriamente compromettere i progressi fatti da tutti noi per ridare fiducia a chi vola”, ha scritto Friend nella lettera. 'La invitiamo caldamente a riprendere in considerazione la reintroduzione di tali oggetti pericolosi (che non dovrebbero stare a bordo di un aereo, in primo luogo) nel nostro ambiente di lavoro'”.

Gli assistenti di volo non stanno valutando la misura di sicurezza in una prospettiva globale. Non stanno cercando di capire quale sia il livello di rischio ottimale, quale genere di compromessi sia accettabile, e quali contromisure permettano di ottenere quel compromesso nei modi più efficaci. Stanno osservando il compromesso dal loro punto di vista: essi ottengono maggiori vantaggi dalla proibizione di oggetti appuntiti rispetto al passeggero medio, perché è il loro ambiente di lavoro, e il costo della misura di sicurezza è sopportato in larga misura dai passeggeri.

Non c'è nulla di sbagliato nel fatto che gli assistenti di volo valutino la sicurezza aerea partendo dalla loro agenda. Sarei sorpreso se non lo

facessero. Ma comprendere l'agenda e le priorità è essenziale per capire come vengono prese le decisioni di sicurezza.

<<http://www.washingtonpost.com/wp-dyn/content/article/2005/08/16/AR2005081601467.html>>

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

\*\* \*\*

## Telecamere di sorveglianza nella metropolitana di New York

New York City sta spendendo 212 milioni di dollari in tecnologie di sorveglianza: 1.000 videocamere e 3.000 sensori di movimento per le stazioni della metropolitana, i ponti e le gallerie della città.

Perché? Perché, visto che le telecamere di sorveglianza non hanno impedito gli attentati di Londra? Perché, visto che non vi è alcuna prova che le telecamere siano efficaci nel ridurre il terrorismo e il crimine, e anzi vi è ogni ragione per credere nella loro totale inefficienza?

Uno dei motivi è che questa è la “minaccia da trama cinematografica” del momento (potete sentire gli echi delle trame da film d'azione quando leggete le varie citazioni dagli articoli di informazione). I terroristi hanno piazzato bombe nella metropolitana di Londra, per cui dobbiamo difendere le nostre metropolitane. Un altro motivo è che le autorità di New York preferiscono eccedere in prudenza. Se non succede niente, sono solo soldi spesi. Ma se accade qualcosa, non potranno mantenere i loro posti di lavoro a meno di non dimostrare di aver fatto tutto il possibile. Le soluzioni tecnologiche fanno sentire tutti meglio.

Se io avessi 212 milioni di dollari da spendere per difendermi dal terrorismo negli USA, non li spenderei per delle telecamere nella metropolitana di New York. Se avessi 212 milioni di dollari per difendere New York dal terrorismo, non li spenderei per delle telecamere nella metropolitana. Questa non è altro che finta sicurezza contro una minaccia da trama cinematografica.

Nota positiva: il denaro servirà anche per realizzare un nuovo sistema di comunicazioni radio per la polizia della metropolitana, e garantirà il servizio di telefonia cellulare nelle stazioni, ma non nelle gallerie.

<<http://www.nytimes.com/2005/08/23/nyregion/23cnd-mta.html>>

<[http://www.washingtonpost.com/wp-dyn/content/article/2005/08/23/AR2005082301488.html?nav=rss\\_technology](http://www.washingtonpost.com/wp-dyn/content/article/2005/08/23/AR2005082301488.html?nav=rss_technology)> oppure <<http://tinyurl.com/ckdst>>

<[http://news.yahoo.com/s/nm/20050823/us\\_nm/security\\_new\\_york\\_dc\\_2&printe](http://news.yahoo.com/s/nm/20050823/us_nm/security_new_york_dc_2&printe)

r=1;\_%20%20ylt=Aij95wnkz9LkKve4ql\_VU8EXIr0F;\_ylu=X3oDMTA3MXN1bHE0BHNIYwN0bWE-> oppure <<http://tinyurl.com/9h9q9>>

<http://it.slashdot.org/it/05/08/23/2237220.shtml?tid=172&tid=215>

L'efficacia delle telecamere:

[http://www.schneier.com/blog/archives/2005/07/surveillance\\_ca.html](http://www.schneier.com/blog/archives/2005/07/surveillance_ca.html)

[http://www.schneier.com/blog/archives/2005/05/surveillance\\_ca\\_1.html](http://www.schneier.com/blog/archives/2005/05/surveillance_ca_1.html)

\*\* \*\*

Le News di Counterpane

Counterpane prende parte al Sourcefire Certified Short Integrator Program

<http://www.counterpane.com/pr-20050824.html>

Teleware è il nuovo partner e rivenditore di servizi di Counterpane in Scandinavia e nel Baltico.

<http://www.counterpane.com/pr-20050822.html>

WilTel Communications annuncia un'alleanza con Counterpane.

<http://www.counterpane.com/pr-20050912.html>

Countermeasure è una newsletter trimestrale che tratta di tecniche per combattere le minacce e proteggere l'integrità dei sistemi in rete. Il primo numero sarà pubblicato il 19. È possibile vedere un'anteprima parziale qui:

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

Schneier intervorrà alla Texas Regional Infrastructure Security Conference in Austin, Texas, il 19 settembre.

<http://www.trisc.org/>

Schneier intervorrà il 20-21 settembre in occasione di eventi organizzati a Columbus e Dayton dalla ACLU.

<http://www.acluohio.org/schneier.htm>

Schneier intervorrà alla ACLU Hawaii Awards Dinner il 25 settembre.

<http://www.acluhawaii.org/>

Schneier intervorrà all'Information Security Forum a Monaco il 10 ottobre.

<http://www.securityforum.org/html/frameset.htm>

\*\* \*\*

Lance Armstrong accusato di doping

Lance Armstrong è stato accusato di essersi servito di una sostanza

proibita durante il Tour de France. Da un punto di vista di sicurezza, questa notizia non è molto interessante. I test sul sangue e sulle urine vengono da sempre utilizzati per rilevare sostanze proibite. L'elemento interessante in questo caso è che il campione di urina è del 1999 e il test è stato compiuto nel 2005.

Nel 1999 non venivano eseguiti test per la droga chiamata EPO. Ora sì. Qualcuno ha preso un vecchio campione di urina (e chi si immaginava che archiviassero vecchi campioni di urina?) e ha effettuato il nuovo test.

Questa possibilità da parte di un meccanismo di sicurezza di andare indietro nel tempo è molto interessante, ed è analoga alla riesumazione di cadaveri richiesta dalle forze dell'ordine per svolgere nuove analisi di patologia legale, o analoga a una nuova tecnica crittografica che permette di leggere messaggi crittografati decenni addietro.

Tale possibilità comporta anche delle gravi implicazioni per quegli atleti che pensano di fare uso di sostanze vietate. Non solo devono eludere i test attuali, ma devono anche pensare a come eludere eventuali test che possano essere inventati in futuro. È facile immaginare atleti a cui vengano annullati i record, le medaglie e i titoli in futuro dopo la scoperta di trasgressioni passate.

D'altra parte, atleti accusati di aver fatto uso di sostanze proibite in passato non hanno molti mezzi per difendersi. Magari inizieranno a conservare campioni del loro sangue e delle loro urine in depositi di sicurezza, anno dopo anno, così da poter avere fluidi puliti e ben conservati coi quali negare le accuse di infrazioni commesse in passato.

<http://www.timesonline.co.uk/article/0,,2094-1753419,00.html>

\*\* \*\*

Peggy Noonan e le minacce terroristiche da trama cinematografica

Peggy Noonan è contraria all'attuale serie di chiusure di basi militari statunitensi perché... beh, perché sostanzialmente crede che possano tornare utili in caso il governo debba proclamare la legge marziale.

Non so nulla di basi militari, né di che cosa dovrebbe rimanere aperto e cosa sia necessario chiudere. Ciò che più mi interessa è come il suo articolo sia un esempio perfetto di un modo di pensare basato su minacce da trama cinematografica.

“Fra le cose che dovremo affrontare nei prossimi dieci anni, come tutti sappiamo, vi è un altro attacco terroristico sul suolo americano. Ma ipotizziamo che il prossimo attacco abbia molti bersagli, e che sia pianificato e coordinato in maniera brillante. Immaginiamo che vi siano già 100 nuclei terroristici importanti negli Stati Uniti, due per stato.

I membri di ogni nucleo sono venuti negli Stati Uniti negli ultimi cinque anni, molti dei quali (ma non tutti) oltrepassando le nostre frontiere. Hanno la loro vita, un impiego, e stanno silenziosamente pianificando l'aggressione.

“Immaginiamo che stiano elaborando un piano di questo tipo: nello stesso giorno di un futuro molto prossimo faranno saltare degli ordigni nucleari nascosti in valigette contemporaneamente in sei diverse città americane, fra cui Washington, che accuserà il colpo maggiore. Centinaia di migliaia di persone potrebbero morire; milioni di vite saranno in pericolo. Le linee di comunicazione saranno disattivate e, come se non bastasse, allo stesso tempo i terroristi lanceranno il più grande attacco cibernetico mai visto, provocando la completa caduta delle comunicazioni e causando grande confusione. Non vi sarà elettricità: centrali elettriche e stazioni di commutazione saranno un altro bersaglio. Non arriverà alcuna comunicazione da Washington, e l'estensione dei danni a livello nazionale sarà ignota quanto sarà evidente quella a livello locale. Vivere quotidianamente diventerà molto difficile, e per mesi vi sarà scarsità di cibo e carburante.

“Immaginiamo uno scenario ancora peggiore. Oltre a tutto questo, il giorno dei bombardamenti, una mezza dozzina di nuclei terroristici si attiverà e ucciderà i leader nazionali, statali e locali. Vi sarà caos, disordini, una diffusa povertà e scarsità di risorse; le forze di polizia, o quel che rimarrà di esse, saranno in minoranza e quindi sopraffatte.

“Così orrendo da rasentare l'impossibile? No, semplicemente orrendo. Da romanzo? Certo. Ma se foste stati un romanziere il 10 settembre 2001 e aveste immaginato una trama in cui due enormi grattacieli sarebbero stati rasi al suolo, il Pentagono sarebbe stato colpito, e la moglie del vice Procuratore Generale degli Stati Uniti avrebbe cercato disperatamente di telefonargli da un aereo commerciale trasformato in un missile; avreste scritto qualcosa di folle e improbabile, che però sarebbe accaduto il giorno dopo.

“Questo naturalmente è soltanto uno dei possibili scenari. Il pazzo che governa la Corea del Nord potrebbe lanciare un attacco missilistico contro gli Stati Uniti domani stesso, e così via. Vi sono possibilità illimitate per la creazione di orribili situazioni”.

Questo gioco dell'“immaginiamo cosa accadrebbe se” è estremamente efficace dal punto di vista emotivo, ma non è affatto il modo di pianificare una linea di condotta per la sicurezza nazionale. C'è una trama da film per giustificare qualsiasi linea di condotta nazionale, e un'altra per rendere inefficace quella stessa linea di condotta.

Noonan scrive: “Queste naturalmente sono soltanto personali congetture. Non ho dati a disposizione per poterle provare”.

Ecco, è esattamente questo il problema.

<http://www.opinionjournal.com/columnists/pnoonan/?id=110007154>

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

## Le buone pratiche del Trusted Computing

Il Trusted Computing Group (TCG) è un consorzio industriale il cui obiettivo è cercare di costruire computer più sicuri. Il gruppo conta moltissimi membri, tuttavia il comitato direttivo è formato da Microsoft, Sony, AMD, Intel, IBM, SUN, HP, e due altre aziende minori che vengono periodicamente elette a rotazione.

L'idea di base è che si costruisca un computer che sia sicuro fin dal principio, con un nucleo hardware "root of trust" chiamato Trusted Platform Module (TPM). Le applicazioni possono girare in sicurezza su tale computer, possono comunicare con altre applicazioni e con i loro proprietari in maniera sicura, e possono garantire che nessun programma "untrusted" possa accedere ai loro dati o al loro codice.

Ciò sembra fantastico, ma è una lama a doppio taglio. Lo stesso sistema che impedisce a worm e virus di propagarsi sul vostro computer può anche impedirvi di utilizzare un qualsiasi software valido ma che non piace al costruttore del vostro hardware o sistema operativo. Lo stesso sistema che proibisce allo spyware di accedere ai vostri file potrebbe anche impedirvi di copiare file audio o video. Lo stesso sistema che verifica che tutte le patch da voi scaricate siano legittime potrebbe anche impedirvi di fare... praticamente qualsiasi cosa.

Lo scorso maggio, il Trusted Computing Group ha pubblicato un documento di best practices (buone pratiche): "Design, Implementation, and Usage Principles for TPM-Based Platforms" [Progettazione, Implementazione e Principi d'Uso per le Piattaforme basate su TPM]. Scritto per utenti e per installatori della tecnologia TCG, il documento cerca di tracciare una linea che separa il buoni e i cattivi impieghi di questa tecnologia.

"I principi che il TCG ritiene stiano alla base di una progettazione, implementazione e utilizzo efficaci, utili e accettabili delle tecnologie TCG sono i seguenti:

"Sicurezza: i componenti abilitati TCG dovranno ottenere un accesso controllato a specifici dati critici assicurati e dovranno misurare e registrare in maniera affidabile le proprietà di sicurezza del sistema. Il meccanismo di registrazione dovrà essere sotto il pieno controllo del proprietario.

"Privacy: i componenti abilitati TCG dovranno essere progettati e implementati tenendo conto della privacy e aderire alla lettera e allo spirito di tutte le linee guida, leggi e norme. Questo comprende, senza

limitarsi ad esse, le Linee Guida OECD, le Fair Information Practices, e la Direttiva Europea per la Protezione dei Dati (95/46/EC).

“Interoperabilità: le implementazioni e le messe in opera delle specifiche TCG dovranno facilitare l’interoperabilità. Inoltre, le implementazioni e le messe in opera delle specifiche TCG non dovranno introdurre nuovi ostacoli all’interoperabilità che abbiano scopo diverso dalla sicurezza.

“Portabilità dei dati: la messa in opera dovrà supportare principi e pratiche prestabiliti di possesso dei dati.

“Controllabilità: ogni proprietario dovrà avere effettive possibilità di scelta e di controllo sull’utilizzo e il funzionamento delle funzioni abilitate TCG che gli appartengono; la sua partecipazione dovrà essere di adesione volontaria. In seguito, qualsiasi utente dovrà essere in grado di disabilitare affidabilmente la funzionalità TCG in modi che non contravvengano alla linea di condotta del proprietario.

“Facilità d’uso: l’utente tecnicamente inesperto dovrà trovare le funzioni abilitate TCG comprensibili e semplici da usare.

Si tratta sostanzialmente di un buon documento, anche se si possono avanzare valide critiche. Mi piace che il documento dichiari espressamente che l’utilizzo coercitivo della tecnologia -- obbligare le persone a usare sistemi per la gestione dei diritti digitali (DRM), per esempio -- non è appropriato: “L’uso di coercizione per imporre a tutti gli effetti l’impiego delle funzionalità TPM non è un uso appropriato della tecnologia TCG”.

Mi piace che il documento cerchi di proteggere la privacy dell’utente: “Tutte le implementazioni di componenti abilitati TCG dovranno garantire che la tecnologia TCG non venga utilizzata in maniera inappropriata per la raccolta di informazioni personali”.

Mi piacerebbe che venisse fatta rispettare l’interoperabilità in maniera più decisa. Il linguaggio utilizzato lascia troppo spazio affinché le aziende pregiudichino l’interoperabilità con il pretesto della sicurezza: “Inoltre, le implementazioni e le messe in opera delle specifiche TCG non dovranno introdurre nuovi ostacoli all’interoperabilità che abbiano scopo diverso dalla sicurezza”.

Suona bene, ma che cosa significa “sicurezza” in tale contesto? Sicurezza dell’utente contro un codice malevolo? Sicurezza dei grandi media contro chi copia musica e video? Sicurezza dei produttori di software contro la concorrenza? Il grosso problema della tecnologia TCG è che può venire utilizzata per conseguire tutti questi tre obiettivi “di sicurezza”, e questo documento dovrebbe definire il concetto di “sicurezza” con maggior precisione.

Critiche a parte, è un buon documento e dovremmo tutti augurarci che venga seguito dalle aziende. L’attenersi alla linea di condotta è

completamente volontario, ma è il tipo di documento che governi e grandi imprese possono prendere come punto di riferimento ed esigere che i produttori vi si attengano.

Ma sta accadendo qualcosa di sospetto. Microsoft sta facendo del suo meglio per impantanare il documento e garantire che non possa essere applicato a Vista (prima conosciuto come Longhorn), il sistema operativo Microsoft di prossima generazione.

La prima stesura del documento risale all'autunno 2003, e ha attraversato il classico processo di revisione agli inizi del 2004. Microsoft ha posticipato l'adozione e la pubblicazione del documento, richiedendo maggiore revisione. Alla fine il documento è stato pubblicato nel giugno di quest'anno (con una data di maggio in copertina).

Nel frattempo il TCG ha realizzato una versione puramente software della specifica: Trusted Network Connect (TNC). Si tratta essenzialmente di un sistema TCG senza un TPM.

Il documento di best practices non si applica a TNC, perché Microsoft (in quanto membro del comitato direttivo del TCG) lo ha bloccato. La scusa è che il documento non era stato scritto pensando ad applicazioni esclusivamente software, perciò non è da applicarsi a sistemi TCG software-only.

Questo è assurdo. Il documento delinea le buone pratiche per come il sistema viene utilizzato. In esso non vi è nulla che spieghi come il sistema funzioni al suo interno. Non vi è nulla di specifico di sistemi basati sull'hardware, nulla che sarebbe differente per sistemi esclusivamente software. Basta leggere il documento e sostituire tutti i riferimenti a "TPM" o a "hardware" con "software" (o, ancor meglio, con "hardware o software"): bastano cinque minuti. Si tratterebbe di una decina di sostituzioni, e nessuna di esse farebbe una sostanziale differenza.

La sola ragione che mi è dato pensare per tutte queste manovre machiavelliche è che il comitato direttivo del TCG stia assicurandosi che il documento non si possa applicare a Vista. Se il documento non viene pubblicato prima del rilascio di Vista, allora ovviamente non si potrà applicare.

Per quel che posso vedere, nessuno sta seguendo questa storia. Nessuno sta domandando perché le buone pratiche del TCG si applicano a sistemi basati sull'hardware se il gruppo sta scrivendo specifiche unicamente software. Nessuno sta domandando perché il documento non si applica a tutti i sistemi TCG, dato che è scritto senza riferirsi ad alcuna specifica tecnologia. Nessuno sta domandando perché il TCG sta rallentando l'adozione di qualsiasi buona pratica riguardante il software.

Credo che le ragioni siano Microsoft e Vista, ma ovviamente occorre svolgere qualche indagine più approfondita.

<http://www.trustedcomputinggroup.org>

Il documento:

[https://www.trustedcomputinggroup.org/downloads/bestpractices/Best\\_Practices\\_Principles\\_Document\\_v1.0.pdf](https://www.trustedcomputinggroup.org/downloads/bestpractices/Best_Practices_Principles_Document_v1.0.pdf) oppure <http://tinyurl.com/cgphx>

Commenti al documento:

<http://cyberlaw.stanford.edu/blogs/bechtold/archives/003155.shtml>

Trusted Network Connect:

<https://www.trustedcomputinggroup.org/downloads/TNC/>

Commenti e confutazioni del mio articolo:

<http://blogs.zdnet.com/Ou/?p=96>

<http://it.slashdot.org/it/05/09/01/1419222.shtml?tid=172&tid=109>

<http://cyberlaw.stanford.edu/blogs/bechtold/archives/003272.shtml>

Ross Anderson sul Trusted Computing:

<http://www.cl.cam.ac.uk/~rja14/tpa-faq.html>

Il mio intervento sul Trusted Computing, ancora quando Microsoft lo chiamava Palladium:

<http://www.schneier.com/crypto-gram-0208.html#1>

Una versione di questo articolo è apparsa originariamente in varie sedi:

[http://news.com.com/Something+fishys+going+on/2010-7350\\_3-5844412.html](http://news.com.com/Something+fishys+going+on/2010-7350_3-5844412.html)

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

[http://news.zdnet.com/2100-1009\\_22-5844520.html](http://news.zdnet.com/2100-1009_22-5844520.html)

<http://www.smh.com.au/articles/2005/09/02/1125302718391.html>

<http://www.theage.com.au/articles/2005/09/02/1125302718391.html>

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

Commenti dei lettori

Da: Stephen Wilson [swilson@lockstep.com.au](mailto:swilson@lockstep.com.au)

Oggetto: Commento sul caso legale in Australia e MD5

Il caso in questione -- purtroppo, forse -- non è stato così tecnico come quanto da lei scritto sullo scorso Crypto-Gram lasciava intendere. Non vi è nulla negli articoli di giornale da lei citati, né a livello di opinione pubblica, che si riferisca alla rottura di MD5. Piuttosto, il caso è stato messo da parte perché i procuratori non sono riusciti a trovare nei tempi assegnati un testimone esperto che potesse parlare a fondo della tecnologia. Per cui è in atto qui un cavillo legale, e non

crittografico!

È interessante notare come questa vicenda dell'autovelox abbia una storia e un precedente. Un anno fa un altro automobilista di Sydney è riuscito a invalidare un altro caso sulla base di un tecnicismo davvero estremo. La legislazione pertinente diceva a quel tempo che il digest code generato dalle telecamere consisteva in “lettere, numeri e simboli”, ma dato che un hash MD5 ha solo lettere e numeri (e non simboli come &%^@#!), l'automobilista ha obiettato che la legge era in errore e che quindi non ci si poteva affidare a quei dispositivi. La legge fu sistemata praticamente da un giorno all'altro per evitare vaghi riferimenti a “simboli”.

Per cui, come può vedere, qui è uno sport fra avvocati quello di trattare la tecnologia degli autovelox sulla base di una serie di tecnicismi e cavilli. Pensi quando scopriranno i “veri” problemi di MD5!

Da: Shachar Shemesh <[shachar@lingnu.com](mailto:shachar@lingnu.com)>

Oggetto: Re: Il profiling e El Al

Ritengo che quanto lei ha affermato essere caratteristico di ciò che El Al sta facendo in merito al “profiling” sia un tantino impreciso. Non è che non traccino profili (stesso discorso per il resto del sistema di difesa israeliano); il fatto è che tracciano un profilo soltanto delle persone che meritano minore attenzione.

In generale, il processo di screening di El Al interroga TUTTI, e con un livello di dettaglio che risulta essere, francamente, imbarazzante. Tuttavia il processo di screening di El Al ha preso alcune decisioni in nome della sicurezza. Il 90% delle persone che volano sulle linee aeree El Al sono cittadini israeliani ebrei. Nella storia dell'aviazione, questa popolazione non è stata responsabile di alcun attacco terroristico. Un selezionatore ebreo di origine israeliana (ovvero la maggioranza degli agenti di sicurezza di El Al) può facilmente capire, senza guardare il passaporto, se qualcuno appartiene o meno a questo gruppo. Per la ragione vista prima, questo gruppo particolare ottiene un trattamento diverso, che si traduce in un interrogatorio meno severo.

La cosa da comprendere è che per aggirare questo profiling, uno non può semplicemente far finta di non appartenere al suo gruppo. Se un arabo israeliano finge di essere un uomo d'affari africano, molto probabilmente verrà interrogato di più, non di meno, proprio perché il suo profilo non quadra. Stesso esteso trattamento se egli riesce a farsi passare per un uomo d'affari cristiano di origine americana. D'altro canto, cercare di farsi passare per un israeliano ebreo difficilmente passerà inosservato, perché un agente di sicurezza sa che aspetto ha un israeliano ebreo, che accento ha, ecc. Per comprendere quanto questo sia il caso, aggiungerò che ogni volta che mi avvicino a uno sportello El Al in qualunque parte del mondo, vengo interpellato in ebraico. Questo

avviene ancor prima che io prenda il passaporto o i biglietti aerei dalla mia borsa.

Questa stessa linea di condotta viene impiegata in molte altre aree. Quando c'è uno stato d'allarme per un possibile attacco terroristico che dovrebbe compiersi, per esempio, a Gaza, non è infrequente chiudere i passaggi fra Gaza e Israele. A causa dell'enorme pressione economica che tale chiusura esercita sulla popolazione palestinese (la maggior parte della quale lavora in Israele), vengono concessi permessi basati sul profiling. All'inizio erano piuttosto ampi (persone sopra i 30 anni sposate con prole, donne, ecc.). A mano a mano che i terroristi trovavano persone all'interno delle "liste bianche", queste furono progressivamente ristrette. Non è stato permesso di passare a persone sposate non perché la sicurezza di Israele ha pensato che fosse impossibile che uno di quel gruppo fosse un terrorista, ma perché fra scegliere di chiudere i passaggi per TUTTI, e chiuderli per una maggioranza, si è preferito lasciar passare qualcuno.

Non mi fraintenda. Sono assolutamente d'accordo con lei che il profiling negli USA è una pessima idea, se fatta in quel modo. Ritengo sia una pessima idea perché le circostanze in America sono molto diverse, e questo rende il profiling statisticamente inefficace, facendo sì che i costi superino di gran lunga i benefici. Se, tuttavia, El Al dovesse iniziare a interrogare CHIUNQUE (ovvero nessun "white profiling"), il prezzo in termini di tempo perso prima del volo e costo del biglietto comporterebbe un livello di sicurezza considerevolmente più basso.

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

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:

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

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

La versione italiana è curata da Communication Valley SpA

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

Per iscriversi o cancellarsi andare all'indirizzo

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

I numeri arretrati sono disponibili all'indirizzo

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

Per informazioni [crypto-gram@communicationvalley.it](mailto:crypto-gram@communicationvalley.it).

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>.

Counterpane Internet Security, Inc. è leader mondiale nel monitoraggio guidato della sicurezza informatica. Gli analisti esperti in sicurezza di Counterpane proteggono reti per aziende inserite nella Fortune 1000 a livello mondiale.

Copyright (c) 2005 by Bruce Schneier.