

CRYPTO-GRAM  
15 ottobre 2009

Scritta da Bruce Schneier  
Chief Security Technology Officer di BT  
e-mail: [schneier@schneier.com](mailto:schneier@schneier.com)  
Web: <<http://www.schneier.com>>

Edizione italiana curata da Communication Valley, Business Unit di Security Reply.  
<<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-0910.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:

- Un dinamitardo... particolare
- News
- La chiusura della sessione di autenticazione
- L'inutilità della difesa degli obiettivi
- Le news su Schneier
- Compromesse le chiavi di firma di Texas Instruments
- Il Canile
- Divulgato il manuale della sicurezza del Ministero della Difesa britannico
- Commenti dei lettori

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

Un dinamitardo... particolare

Non ditelo alla TSA, ma il mese scorso qualcuno ha cercato di assassinare un principe saudita facendo esplodere un ordigno sistemato nel proprio retto. Si è finto un militante pentito, mentre in realtà era un cavallo di troia: "La detonazione ha fatto completamente a pezzi al-Asiri ma ha ferito soltanto superficialmente il principe, che era l'obiettivo del fallito tentativo di assassinio da parte di al-Asiri".

Per anni ho fatto questa battuta su Richard Reid: "Ringraziamo il fatto che si trattava del dinamitardo delle scarpe e non delle mutande". Ora ne abbiamo tristemente un esempio.

Lewis Page, un "operatore esperto nell'eliminazione di ordigni improvvisati che ha collaborato con la polizia continentale britannica dal 2001 al 2004", ha fatto notare come tale minaccia sia in realtà poco efficace per tre ragioni: 1) Non è possibile infilare una grande quantità di esplosivo all'interno di una cavità del corpo umano, 2) la detonazione è un tantino problematica, e 3) un corpo umano può attenuare un'esplosione in maniera assai efficace (si pensi a una persona che si butta su una granata per salvare i propri amici).

Ma chi ha mai accusato la TSA di essere razionale?

<[http://www.stratfor.com/weekly/20090902\\_aqap\\_paradigm\\_shifts\\_and\\_lessons\\_learned](http://www.stratfor.com/weekly/20090902_aqap_paradigm_shifts_and_lessons_learned)>

oppure <<http://tinyurl.com/ye9rdqg>>

<<http://timesofindia.indiatimes.com/articleshow/msid-4951665,prtpage-1.cms>>

oppure <<http://tinyurl.com/ybxvm5q>>

<<http://www.stuff.co.nz/sunday-star-times/news/world/2833157/Bomb-in-anal-cavity-raises-new-airline-concern>>

oppure <<http://tinyurl.com/na7rbd>>

<<http://homelandsecuritynewswire.com/single.php?id=8705>>

<<http://www.hlswatch.com/2009/09/18/anal-secrets-and-the-coming-tempest-in-homeland-security/>>

oppure <<http://tinyurl.com/yds7vwg>>

Una pagina sulla fattibilità di questa tattica:

<[http://www.theregister.co.uk/2009/09/21/bum\\_bombing/](http://www.theregister.co.uk/2009/09/21/bum_bombing/)>

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

News

Stampare le chiavi delle manette in dotazione alla polizia utilizzando una stampante 3D:

<<http://blackbag.nl/?p=940>>

<[http://www.schneier.com/blog/archives/2009/09/printing\\_police.html#c393047](http://www.schneier.com/blog/archives/2009/09/printing_police.html#c393047)>

oppure <<http://tinyurl.com/yf66534>>

<[http://www.schneier.com/blog/archives/2009/09/printing\\_police.html#c393012](http://www.schneier.com/blog/archives/2009/09/printing_police.html#c393012)>

oppure <<http://tinyurl.com/yf6cj5e>>

Il Dipartimento per la Sicurezza Nazionale sta pensando di modificare il sistema di allerta codificato a colori -- quel sistema inutile e preso in giro da tutti -- eliminando due dei cinque livelli di allarme. Spero che vi sentirete tutti più al sicuro adesso.

<[http://www.schneier.com/blog/archives/2009/09/modifying\\_the\\_c.html](http://www.schneier.com/blog/archives/2009/09/modifying_the_c.html)>

Ottimo articolo sui "rifugi terroristici", come l'Afghanistan, e sul perché non rappresentano quella gran minaccia che sarebbero secondo certuni.

<<http://www.washingtonpost.com/wp-dyn/content/article/2009/09/15/AR2009091502977.html?wpisrc=newsletter>>  
oppure <<http://tinyurl.com/mvqc2c>>

Dedurre relazioni di amicizia dai dati di posizionamento geografico:  
<[http://www.schneier.com/blog/archives/2009/09/inferring\\_friend.html](http://www.schneier.com/blog/archives/2009/09/inferring_friend.html)>

Nel 2005 parlai dell'inefficacia dell'autenticazione a due fattori come metodo per mitigare le frodi bancarie. Adesso stiamo assistendo ad attacchi che aggirano proprio quella misura di sicurezza.  
<[http://www.schneier.com/blog/archives/2009/09/hacking\\_two-fac.html](http://www.schneier.com/blog/archives/2009/09/hacking_two-fac.html)>

Un calcolatore quantico fattorizza il numero 15. È uno sviluppo importante, ma non si abbandoni la crittografia a chiave pubblica tanto presto.  
<[http://www.schneier.com/blog/archives/2009/09/quantum\\_compute.html](http://www.schneier.com/blog/archives/2009/09/quantum_compute.html)>

Questa è una buona cosa: "Una corte distrettuale dell'Illinois ha permesso a una coppia di denunciare la loro banca per non essere stata in grado di proteggere adeguatamente il loro conto corrente, dopo che un hacker non identificato ha ottenuto un prestito di 26.500 dollari sul conto servendosi del nome utente e della password dei due clienti". Come ho già scritto in precedenza, si tratta dell'unico sistema per attenuare questo genere di frode. È un principio di sicurezza molto importante: assicurarsi che la persona che ha il potere di mitigare il rischio sia responsabile per il rischio. In questo caso i titolari del conto corrente non avevano nulla a che fare con la sicurezza del loro conto. Non potevano sottoporlo ad auditing. Non potevano migliorare la sicurezza. La banca, invece, ha la possibilità di migliorare la sicurezza e attenuare i rischi, ma dato che scarica i costi sui propri clienti, non ha alcun incentivo a farlo. Cause legali come questa hanno la possibilità di rimediare all'esternalità e migliorare la sicurezza.  
<[http://www.schneier.com/blog/archives/2009/09/eliminating\\_the.html](http://www.schneier.com/blog/archives/2009/09/eliminating_the.html)>

Maggiori informazioni sulle scatole di Monopoli contenenti informazioni segrete per la fuga che venivano passate ai prigionieri di guerra della Seconda Guerra Mondiale:  
<<http://www.abcnews.go.com/Technology/monopolys-hidden-maps-wwii-pows-escape/story?id=8605905>>  
oppure <<http://tinyurl.com/lcjxut>>  
<[http://www.schneier.com/blog/archives/2007/12/monopoly\\_sets\\_w.html](http://www.schneier.com/blog/archives/2007/12/monopoly_sets_w.html)>

Sears spia i propri clienti; non sono solo gli hacker a rubare informazioni sanitarie e finanziarie.  
<<http://www.walletpop.com/blog/2009/09/14/sears-gets-a-gentle-touch-to-the-wrist-for-allegedly-spying-on-i/>>  
oppure <<http://tinyurl.com/nznrnu>>

La faccenda Sears mi fa venire in mente del rootkit di Sony nel 2005, il quale, strano ma vero, è tornato a far parlare di sé:  
<<http://torrentfreak.com/retailer-must-compensate-sony-anti-piracy-rootkit-victim-090914/>>  
oppure <<http://tinyurl.com/o7j7qs>>

Da The Onion: "Le autorità sono state chiamate per esaminare un prosciutto dall'aria sospetta":  
<[http://www.theonion.com/content/radio\\_news/authorities\\_called\\_in\\_to](http://www.theonion.com/content/radio_news/authorities_called_in_to)>

Una guida a vignette per capire AES.

<<http://www.moserware.com/2009/09/stick-figure-guide-to-advanced.html>>

Predire le caratteristiche di una persona dalla compagnia che frequenta:

<[http://www.schneier.com/blog/archives/2009/09/predicting\\_char.html](http://www.schneier.com/blog/archives/2009/09/predicting_char.html)>

Il cittadino americano medio commette tre reati al giorno: è il titolo di nuovo libro scritto da Harvey Silverglate. Nello specifico, il problema nasce dall'intersezione di leggi poco chiare e della tecnologia che si muove a gran velocità.

<[http://www.schneier.com/blog/archives/2009/09/the\\_problem\\_of.html](http://www.schneier.com/blog/archives/2009/09/the_problem_of.html)>

L'immediatezza influisce sulle valutazioni dei rischi:

<<http://www.sciencedaily.com/releases/2009/09/090923102405.htm>>

In Svezia, durante un'audace rapina a una banca in cui è stato utilizzato anche un elicottero, i malviventi hanno neutralizzato un elicottero della polizia piazzando un pacco con la scritta "bomba" accanto all'hangar; in questo modo hanno innescato tutte le procedure di sicurezza e di evacuazione come diversivo mentre loro fuggivano. L'attacco ha funzionato, malgrado la polizia fosse stata avvertita.

<<http://news.bbc.co.uk/2/hi/europe/8270619.stm>>

<<http://www.youtube.com/watch?v=Bgc0NrI6iv0>>

<<http://www.thelocal.se/22260/20090924/>>

<<http://www.stockholmnews.com/more.aspx?NID=4044>>

Riprodurre chiavi da fotografie scattate a distanza e da angoli diversi:

<<http://vision.ucsd.edu/~blaxton/sneakey.html>>

Quelli di voi che si portano appresso le chiavi lasciandole penzolare dalla cintura dei pantaloni, prendano nota.

Provare la correttezza di un programma informatico:

<[http://www.schneier.com/blog/archives/2009/10/proving\\_a\\_compu.html](http://www.schneier.com/blog/archives/2009/10/proving_a_compu.html)>

Messinscena di sicurezza a New York in occasione dell'Assemblea Generale delle Nazioni Unite:

<[http://politics.theatlantic.com/2009/09/for\\_those\\_entranced\\_by\\_security.php](http://politics.theatlantic.com/2009/09/for_those_entranced_by_security.php)>

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

Se eravate curiosi di sapere ciò che il Dipartimento per la Sicurezza Nazionale sa di voi, ecco una vera registrazione degli spostamenti di una persona effettuata dal Dipartimento per la Sicurezza Nazionale.

<<http://philosecurity.org/2009/09/07/what-does-dhs-know-about-you>>

Spostare ippopotami nell'epoca post-11 settembre:

<[http://www.schneier.com/blog/archives/2009/10/moving\\_hippos\\_i.html](http://www.schneier.com/blog/archives/2009/10/moving_hippos_i.html)>

Esiste un Trojan che non solo effettua transazioni a vostro nome sul vostro conto corrente, ma altera le ricevute bancarie in modo che non vi accorgiate delle movimentazioni dei fondi. Se c'è una morale in tutto questo è che le banche non possono affidarsi ai clienti per scoprire le frodi. Ma lo si sapeva già.

<<http://www.wired.com/threatlevel/2009/09/rogue-bank-statements/>>

<<http://news.bbc.co.uk/2/hi/technology/8271384.stm>>

Questo dovrebbe essere un consiglio più che ovvio: non lasciar riprogrammare i computer del penitenziario da detenuti esperti in informatica. Ma del resto stiamo parlando della stessa prigione che ha dato accesso alle proprie chiavi a un detenuto esperto scassinatore. Quale sarà la prossima mossa: detenuti cecchini incaricati di sorvegliare l'armeria?

<<http://www.mirror.co.uk/news/top-stories/2009/09/27/computer-meltdown-115875-21703149/>>

oppure <<http://tinyurl.com/yedoph2>>

I testimoni oculari sono più precisi nell'identificare i criminali quando vengono assistiti da un computer più che da agenti di polizia.

<<http://www.newscientist.com/article/mg20327275.500-virtual-cop-to-run-identity-parades.html>>

oppure <<http://tinyurl.com/yaoa86l>>

Rilevazione comportamentale: individuare soggetti intenzionati a far del male:

<[http://www.boston.com/news/science/articles/2009/09/18/spotting\\_a\\_terrorist/](http://www.boston.com/news/science/articles/2009/09/18/spotting_a_terrorist/)>

oppure <<http://tinyurl.com/o6pajr>>

Una truffa interessante per accedere alla cassetta di sicurezza di un albergo:

<[http://www.schneier.com/blog/archives/2009/10/hotel\\_safe\\_scam.html](http://www.schneier.com/blog/archives/2009/10/hotel_safe_scam.html)>

Rilevare firme falsificate analizzando la pressione della penna e l'angolazione della scrittura:

<[http://www.schneier.com/blog/archives/2009/10/detecting\\_forge.html](http://www.schneier.com/blog/archives/2009/10/detecting_forge.html)>

Qualche settimana fa il Segretario del Dipartimento per la Sicurezza Nazionale Janet Napolitano ha dichiarato che gli Stati Uniti avevano bisogno di assumere un migliaio di esperti di sicurezza cibernetica nel giro dei prossimi tre anni. Bob Cringely dubita persino che esistano 1.000 esperti di sicurezza cibernetica in circolazione. Suppongo che dipenda da quel che Napolitano intende per 'esperti'.

<<http://www.cnn.com/2009/POLITICS/10/02/dhs.cybersecurity.jobs/>>

<<http://www.cringely.com/2009/10/the-cybersecurity-myth/>>

Maiali che neutralizzano i sistemi di alimentazione basati su RFID:

<[http://www.youtube.com/watch?v=8ImZmDYme\\_s](http://www.youtube.com/watch?v=8ImZmDYme_s)>

Utilizzare il wi-fi per 'vedere' attraverso i muri:

<<http://www.wired.com/threatlevel/2009/10/see-through-walls/>>

Wi-fi blocking paint:

<<http://news.bbc.co.uk/2/hi/technology/8279549.stm>>

Ottimo studio di David Dittrich: "Malware to crimeware: How far have they gone, and how do we catch up?" (Dal malware al crimeware: quanti progressi hanno compiuto i criminali, e come fare per recuperare lo svantaggio?).

<<http://staff.washington.edu/dittrich/papers/dittrich-login0809.pdf>>

P versus NP: lo stato delle cose:

<<http://cacm.acm.org/magazines/2009/9/38904-the-status-of-the-p-versus-np-problem/fulltext>>

oppure <<http://tinyurl.com/n9amud>>

Steganografia del 1777.

<<http://www.lettersofnote.com/2009/10/masked-letter.html>>

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

La chiusura della sessione di autenticazione

Nella sicurezza informatica si compiono molti sforzi per cercare di risolvere il problema dell'autenticazione. Che siano password, token di sicurezza, domande segrete, immagini da memorizzare o altro ancora, gli ingegneri continuano a inventare metodi sempre più complicati (e, si spera, più sicuri) perché gli utenti possano dimostrare la propria identità in Internet.

Si tratta di cose molto importanti, come ben sa chiunque abbia un conto bancario online o una rete aziendale remota. Ma non è stato mai compiuto molto lavoro per affrontare l'altro estremo del problema: come dire al sistema all'altro capo della linea che ci siamo scollegati? Come 'disautenticarsi' e chiudere la sessione?

Il mio computer a casa, quando voglio chiudere la sessione, richiede un logout o lo spegnimento della macchina. Questo metodo con me funziona perché ne so abbastanza per effettuare l'operazione, ma molte persone quando si allontanano dal proprio computer spesso lo lasciano acceso. Di conseguenza molti computer negli uffici vengono lasciati con una sessione attiva quando gli impiegati vanno a pranzo o quando tornano a casa la sera. Ovviamente si tratta di una vulnerabilità di sicurezza.

Il metodo più comune per affrontare il problema è far sì che il sistema vada in timeout. Posso ordinare al mio computer di chiudere la mia sessione automaticamente dopo un certo periodo di inattività -- cinque minuti, per esempio. Serve qualche aggiustamento, tuttavia, per perfezionare questo sistema. Se si effettua la disconnessione dalla sessione troppo presto, l'utente si arrabbierà; se si aspetta troppo tempo, il sistema potrebbe essere vulnerabile in quell'arco temporale. Il mio server email aziendale mi chiude la sessione dopo circa dieci minuti, e la cosa mi infastidisce in continuazione.

In alcuni sistemi è stato sperimentato un token: un token di autenticazione USB che deve essere inserito per far funzionare il computer, oppure un token RFID che effettua automaticamente il logout di un utente quando il token si sposta oltre una certa distanza dal computer. Naturalmente gli impiegati tenderanno a lasciare il token inserito nei loro computer tutto il tempo; ma se lo si attacca alle loro chiavi dell'auto o al badge che devono avere sempre con sé in ufficio, i rischi vengono ridotti.

Però è un metodo costoso. Un progetto di ricerca si è servito di un dispositivo Bluetooth, come un telefono cellulare, e misurava la vicinanza al computer. Il sistema poteva essere programmato per bloccare il computer se quel dispositivo Bluetooth usciva dal raggio di riconoscimento.

Alcuni sistemi chiudono la sessione di autenticazione al termine di ogni transazione. Ciò non funzionerebbe con i computer, ma può andar bene per gli sportelli Bancomat. La macchina sputa la mia carta prima di darmi il contante, oppure richiede semplicemente

una passata della carta e si assicura che io la estragga dalla macchina. Se voglio effettuare un'altra transazione devo reinserire la carta e immettere il PIN una seconda volta.

Vi è un'analogia fisica che tutti possono spiegare: le serrature delle porte. La vostra porta di casa si blocca alle vostre spalle quando la chiudete, o è necessario che la chiudiate a chiave manualmente? Nel primo caso abbiamo un sistema che effettua automaticamente il logout della vostra sessione, mentre nel secondo caso è necessario eseguire il logout manualmente. Si vendono e si utilizzano entrambi i tipi di serratura: quale scegliete dipende sia da come usate la porta e da chi vi aspettate un tentativo di intrusione.

Progettare sistemi considerando l'usabilità è difficile, specialmente quando entra in gioco la sicurezza. Quasi per definizione, rendere qualcosa più sicuro lo rende meno usabile. Scegliere un metodo di autenticazione dipende molto da come viene impiegato un sistema e dal modello di minaccia. Occorre bilanciare l'aumento di sicurezza da una parte e l'arrabbiatura degli utenti dall'altra, e trovare il giusto equilibrio richiede tempo e una serie di prove, ed è più un'arte che una scienza.

Logout automatico:

<[http://www.schneier.com/blog/archives/2009/06/protecting\\_agai.html](http://www.schneier.com/blog/archives/2009/06/protecting_agai.html)>

Logout per prossimità:

<<http://www.matthew.ath.cx/projects/bluemon/>>

Questo articolo è originariamente apparso su ThreatPost.

<<http://threatpost.com/blogs/difficulty-un-authentication-128>>

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

L'inutilità della difesa degli obiettivi

Questa è semplicemente un'idiozia:

"Il Beaver Stadium è un obiettivo terroristico. Molto probabilmente si tratta dell'obiettivo numero uno della regione. In quanto tale, ha diritto a misure di sicurezza adeguate, ma sta forse ottenendo tale sicurezza?

[...]

"Quando lo stadio non viene utilizzato non significa che cessi di essere un obiettivo. Deve venire sottoposto a una sorveglianza costante. Una semplice soluzione è quella di impiegare agenti di polizia 24 ore al giorno, sette giorni alla settimana. È in questo modo che è stato sventato un complotto per distruggere il ponte di Brooklyn: con la presenza della polizia. Anche se è un'operazione dai costi significativi, tali costi non sono nulla in confronto a quel che si pagherebbe se lo stadio fosse distrutto o danneggiato.

“L’idea è quella di creare onnipresenza, in modo che tutti (compresi i terroristi e i buontemponi) credano che lo stadio venga costantemente vigilato al punto che ogni tentativo distruttivo sarebbe inutile”.

In realtà il complotto del ponte di Brooklyn è fallito perché i cospiratori erano degli imbecilli e il piano stesso (tagliare i cavi con una fiamma ossidrica) era stupido. Quello, più il classico informatore della polizia che li ha incitati.

Ma lasciamo perdere. Il Beaver Stadium è lo stadio di football americano della Pennsylvania State University, e questo articolo sostiene che sia un potenziale bersaglio terroristico e che debba essere protetto dalla polizia 24 ore su 24, 7 giorni su 7.

Il problema di questo modo di ragionare è che è insensato. Come ho scritto in un articolo che apparirà sul “New Internationalist”:

“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 in un grande paese vi sono letteralmente milioni di bersagli potenziali (solo negli Stati Uniti vi sono cinque milioni di edifici commerciali), e centinaia di potenziali tattiche terroristiche; è impossibile difendere tutti i luoghi da ogni possibile minaccia, ed è impossibile prevedere quale tattica e quale bersaglio sceglieranno i terroristi per il prossimo attacco.”.

Difendere i singoli bersagli ha senso soltanto se il numero dei bersagli potenziali è basso. Se esistessero sette bersagli terroristici e ne difendessimo cinque, ridurremmo drasticamente la capacità dei terroristi di fare danni. Ma se vi sono milioni di bersagli terroristici e ne difendiamo cinque, i terroristi neanche se ne accorgono. In genere non mi piacciono quelle misure di sicurezza che riescono soltanto a far deviare leggermente i terroristi dai loro piani.

Per non parlare della spesa, che sarebbe enorme. Aggiungiamo questi bersagli terroristici secondari -- stadi, cinema, chiese, scuole, centri commerciali, uffici, qualunque luogo pubblico affollato -- e si arriva ad altri duecentomila bersagli, Beaver Stadium compreso. Una protezione a tempo pieno da parte delle forze di polizia richiede uomini, per cui facciamo un milione di poliziotti. Calcoliamo 100.000 dollari a poliziotto ogni anno (probabilmente una stima per difetto), e abbiamo un costo annuo totale di 100 miliardi di dollari (più o meno quel che stiamo spendendo ogni anno in Iraq). D’altro canto, assumere un americano su trecento per fargli sorvegliare la nostra infrastruttura risolverebbe il problema della disoccupazione. E dato che i poliziotti ricevono assistenza sanitaria, si risolverebbe anche il problema della sanità. Si faccia attenzione almeno a non assumere per sbaglio un terrorista per proteggerci dai terroristi -- sarebbe imbarazzante.

Tutta l’idea è priva di senso. Come dico da anni, quel che funziona è l’investigazione, l’intelligence e la risposta alle emergenze:

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, e come favorisce od ostacola il terrorismo.

L'articolo sul Beaver Stadium:

<<http://www.centredaily.com/opinion/story/1548830.html>>

Il ritratto del terrorista moderno da idiota:

<<http://www.schneier.com/essay-174.html>>

Gli informatori:

<<http://www.cbsnews.com/stories/2009/05/22/opinion/main5034353.shtml>>

Il mio articolo sull'investigazione, l'intelligence e la risposta alle emergenze:

<<http://www.schneier.com/essay-087.html>>

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

Le news su Schneier

Interverrò all'Information Security Decisions a Chicago il 21 ottobre.

<<http://infosecuritydecisions.techtarget.com/infosecuritydecisions/html/index.html>>

oppure <<http://tinyurl.com/ygqwx8l>>

Interverrò al 4th International Workshop on Security a Toyama, in Giappone, il 28 ottobre.

<<http://www.iwsec.org/2009/>>

Interverrò all'ISF Annual World Congress a Vancouver il 2 novembre.

<<https://www.securityforum.org/html/congres.htm>>

Interverrò alla Gartner Identity and Access Management Conference a San Diego il 9 novembre.

<<http://www.gartner.com/it/page.jsp?id=838920>>

Interverrò all'Internet Governance Forum a Sharm el-Sheikh, in Egitto, il 15 novembre.

<<http://igf09.eg/home.html>>

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

Compromesse le chiavi di firma di Texas Instruments

Le calcolatrici Texas Instruments fanno uso di firme digitali RSA per autenticare gli aggiornamenti del loro sistema operativo. Sfortunatamente le loro chiavi di firma sono troppo corte: 512 bit. Qualche settimana fa, uno sforzo congiunto ha permesso di

fattorizzare i moduli e di pubblicare le chiavi private. Texas Instruments ha risposto minacciando con il DMCA i siti Web che hanno pubblicato le chiavi, ma è troppo tardi.

Per ora siamo in possesso delle chiavi private dei sistemi operativi dei seguenti modelli: TI-92+, TI-73, TI-89, TI-83+/TI-83+ Silver Edition, Voyage 200, TI-89 Titanium e TI-84+/TI-84 Silver Edition, nonché del date-stamp della chiave di firma dei modelli TI-73, Explorer, TI-83 Plus, TI-83 Silver Edition, TI-84 Plus, TI-84 Silver Edition, TI-89, TI-89 Titanium, TI-92 Plus e Voyage 200.

Morale: mai assumere che se la propria applicazione è poco conosciuta, o se non esiste un incentivo economico ovvio per farlo, che la propria crittografia non venga compromessa se si utilizzano chiavi troppo corte.

<<http://www.ticalc.org/archives/news/articles/14/145/145273.html>>  
<[http://wikileaks.org/wiki/Suppressed\\_Texas\\_Instruments\\_cryptographic\\_signing\\_keys,\\_28\\_Aug\\_2009](http://wikileaks.org/wiki/Suppressed_Texas_Instruments_cryptographic_signing_keys,_28_Aug_2009)>  
oppure <<http://tinyurl.com/nrorec>>  
<<http://www.ticalc.org/archives/news/articles/14/145/145316.html>>  
<[http://en.wikipedia.org/wiki/Texas\\_Instruments\\_signing\\_key\\_controversy](http://en.wikipedia.org/wiki/Texas_Instruments_signing_key_controversy)>  
<<http://diomedes.phear.cc/~chronomex/keys.shtml>>  
<<http://88.80.16.63/leak/ti-os-keys-dmca-2009.txt>>

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

Il Canile

Due proposte questa volta.

Crypteto:

<[http://www.schneier.com/blog/archives/2009/09/the\\_doghouse\\_cr.html](http://www.schneier.com/blog/archives/2009/09/the_doghouse_cr.html)>

Privacy Inside:

<[http://www.schneier.com/blog/archives/2009/10/the\\_doghouse\\_pr\\_1.html](http://www.schneier.com/blog/archives/2009/10/the_doghouse_pr_1.html)>

Entrambe molto divertenti da leggere.

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

Divulgato il manuale della sicurezza del Ministero della Difesa britannico

Consta di più di 2.000 pagine, per cui ci vorrà del tempo prima di poter ricavare qualcosa. Secondo Ross Anderson, che gli ha dato una rapida occhiata, "sembra essere l'equivalente burocratico di un programma per computer completamente incasinato: un guazzabuglio di cose scritte da persone provenienti da background diversi, con livelli diversi di conoscenze, in epoche diverse".

La parte riguardante la sicurezza informatica inizia da pagina 1.531.

<[http://www.wikileaks.org/wiki/UK MoD Manual of Security Volumes 1%2C 2 and 3 Issue 2%2C JSP-440%2C RESTRICTED%2C 2389 pages%2C 2001](http://www.wikileaks.org/wiki/UK_MoD_Manual_of_Security_Volumes_1%2C_2_and_3_Issue_2%2C_JSP-440%2C_RESTRICTED%2C_2389_pages%2C_2001)>

oppure <<http://tinyurl.com/ybc4yxj>>

<[http://www.theregister.co.uk/2009/10/05/leaked\\_defence\\_manual/](http://www.theregister.co.uk/2009/10/05/leaked_defence_manual/)>

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

Commenti dei lettori

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

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

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

Dal 1998 CRYPTO-GRAM è una newsletter mensile gratuita che offre riassunti, analisi, approfondimenti, e commenti sulla sicurezza (informatica e in generale) e sulla crittografia. I numeri arretrati sono disponibili all'indirizzo <<http://www.schneier.com/crypto-gram.html>>. Per iscriversi, cancellare l'iscrizione o cambiare il proprio indirizzo a cui recapitare la newsletter, visitate sempre <<http://www.schneier.com/crypto-gram.html>>

La versione italiana è curata da Communication Valley, Business Unit di Security Reply. <<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)

I commenti a CRYPTO-GRAM devono essere inviati a [schneier@counterpane.com](mailto: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) 2009 - Bruce Schneier.