

CRYPTO-GRAM
15 ottobre 2004

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

Edizione italiana curata da Communication Valley SpA

E-mail: schneier@counterpane.com

Web: <<http://www.schneier.com>> oppure <<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>>

** **

In questo numero:

Nuovo Blog, e qualche cambiamento per Crypto- Gram
Mantenere segrete le interruzioni di un servizio
I passaporti RFID
Delle scritte in arabo bastano ad interrompere un volo
Le ristampe di Crypto- Gram
News
Le News di Counterpane
L'eredità del DES
Il Canile: Lexar JumpDrives
Gli scanner di targhe automobilistiche e la privacy
La libertà accademica e la sicurezza
Commenti dei lettori

** **

Nuovo Blog, e qualche cambiamento per Crypto- Gram

Sto per apportare diversi cambiamenti a Crypto- Gram, tutti al fine di dare ai lettori maggiori opzioni di consultazione.

Blog: Crypto- Gram è ora disponibile in forma di blog. Intitolato "Schneier on Security", il blog avrà gli stessi contenuti di Crypto- Gram, ma verranno pubblicati continuamente e non solo il 15 di ogni mese. Inizialmente, i commenti al blog non saranno attivi: li abiliterò non appena il mio software anti- spam per i blog sarà in funzione.

RSS: Il formato RSS di Crypto- Gram è attivo da sei mesi ormai. Chi si è iscritto al RSS riceverà la versione blog di Crypto- Gram invece di quella mensile.

E-Mail: Crypto- Gram sarà ancora disponibile sotto forma di e-mail mensile, e i numeri arretrati di Crypto- Gram saranno ancora consultabili sul Web.

Da questo momento fino al prossimo numero della newsletter, la mailing list verrà spostata su schneier.com, con un nuovo software, per cui cambieranno le istruzioni per iscriversi e per cancellare l'iscrizione. Se dovete iscrivervi o disiscrivervi durante questo periodo, la pagina di Crypto- Gram

<http://www.schneier.com/blog/archives/2004/10/rfid_passports.html>

Dall'11 settembre 2001, l'amministrazione Bush e, nello specifico, il Dipartimento per la Sicurezza Nazionale, ha voluto che il mondo si standardizzasse adottando passaporti leggibili mediante appositi dispositivi. I prossimi passaporti statunitensi (ora in fase sperimentale) incorporeranno un chip che permetterà al passaporto di contenere un maggior numero di informazioni rispetto a semplici scritte leggibili da una macchina e permetterà agli ufficiali di frontiera di leggere rapidamente e con facilità quelle informazioni. Questi sono requisiti più che ragionevoli e costituiscono una buona idea per portare finalmente la tecnologia dei passaporti nel XXI secolo. Ma la pessima cosa è che l'amministrazione sta sostenendo l'impiego di chip per l'identificazione mediante radiofrequenze (RFID), sia per i passaporti americani che per quelli esteri.

I chip RFID sono come le smart card, ma possono essere letti a distanza. Un dispositivo di ricezione può "parlare" al chip in remoto, senza alcun bisogno di contatto fisico, e ottenere qualsiasi informazione in esso contenuta. Gli ufficiali di controllo stimano di poter scaricare le informazioni sul chip semplicemente tenendolo a pochi centimetri di distanza da un lettore.

Purtroppo, i chip RFID possono essere letti da qualsiasi lettore, non solo da quelli presenti ai posti di controllo. Il risultato di tutto questo è che chiunque abbia con sé un passaporto RFID sta trasmettendo e diffondendo la propria identità.

Pensate per un momento a cosa comporta tutto ciò. Significa che il proprietario del passaporto sta continuamente trasmettendo il proprio nome, nazionalità, età, indirizzo e qualsiasi altro dato presente sul chip RFID. Significa che chiunque abbia un lettore può ottenere quelle informazioni senza che il proprietario del passaporto lo sappia e lo permetta. Significa che borseggiatori, rapitori e terroristi possono facilmente (e di nascosto) individuare cittadini americani all'interno di una folla.

È una chiara minaccia sia per la privacy che per la sicurezza personale. In parole povere, una pessima idea.

L'amministrazione sostiene che i chip possono essere letti solo a una distanza di pochi centimetri, per cui non esiste possibilità di abusi. Ma questa è una dichiarazione mostruosamente ingenua. Tutti i protocolli wireless possono funzionare a distanze maggiori di quelle specificate. Durante i test, i chip RFID sono stati letti a 20 metri di distanza e i miglioramenti in campo tecnologico sono inevitabili.

La sicurezza è sempre un compromesso e un bilanciamento. Se i benefici apportati dai chip RFID sono superiori ai rischi, allora forse vale la pena di impiegarli. Di certo non c'è questo gran beneficio quando una persona presenta il passaporto a un ufficiale di frontiera. Se quell'ufficiale deve prendere il passaporto e portarlo vicino a un lettore, cosa gli impedisce di avvicinarsi qualche centimetro in più, che è quanto richiesto dai chip "a contatto"?

L'amministrazione sta deliberatamente scegliendo una tecnologia meno sicura senza alcuna giustificazione. Se ci fosse un valido motivo per preferire quella tecnologia, allora potrebbe avere senso, ma non c'è. Vi sono enormi costi in quanto a sicurezza e privacy e nessun beneficio. Una qualsiasi analisi razionale arriverà alla conclusione per cui non esiste alcun motivo per preferire un chip RFID a un chip convenzionale.

Purtroppo una ragione c'è. Almeno, è l'unica ragione che mi sia venuta in mente del perché l'amministrazione voglia i chip RFID nei passaporti: per avere essa stessa un accesso segreto. Vogliono essere in grado di identificare le persone in una folla, vogliono poter distinguere gli stranieri dagli americani. Vogliono poter fare proprio quello che (malgrado chiare dimostrazioni del contrario) insistono non possa essere fatto.

In genere sono molto cauto nell'ascrivere ad un'agenzia governativa certe losche manovre. L'incompetenza è la norma e la malevolenza è molto rara. Ma questo mi pare il classico caso in cui il governo mette i propri interessi sopra la sicurezza e la privacy dei propri cittadini, per poi uscirsene con chiare menzogne a riguardo.

Le ristampe di Crypto- Gram

Crypto- Gram è attualmente al suo settimo 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.

Il futuro della sorveglianza:

<<http://www.schneier.com/crypto-gram-0310.html#1>> (originale)
<<http://www.cryptogram.it/ottobre03.htm#a1>> (traduzione)

La strategia nazionale per rendere sicuro il Cyberspazio:

<<http://www.schneier.com/crypto-gram-0210.html#1>>
<<http://www.cryptogram.it/ottobre02.htm#a1>>

Cyber- terrorismo:

<<http://www.schneier.com/crypto-gram-0110.html#1>>
<<http://www.cryptogram.it/ottobre01.htm#a1>>

I pericoli della porta 80:

<<http://www.schneier.com/crypto-gram-0110.html#9>>
<<http://www.cryptogram.it/ottobre03.htm#a1>>

Attacchi semantici:

<<http://www.schneier.com/crypto-gram-0010.html#1>>

La NSA sulla sicurezza:

<<http://www.schneier.com/crypto-gram-0010.html#7>>

“Così vorresti diventare un crittografo”:

<<http://www.schneier.com/crypto-gram-9910.html#SoYouWanttoBeaCryptographer>>

Lunghezza delle chiavi e sicurezza:

<<http://www.schneier.com/crypto-gram-9910.html#KeyLengthandSecurity>>

Steganografia: verità e fantasie:

<<http://www.schneier.com/crypto-gram-9810.html#steganography>>

Appunti per gli apprendisti scrittori di cifrati:

<<http://www.schneier.com/crypto-gram-9810.html#cipherdesign>>

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

News

<<http://www.schneier.com/blog/archives/2004/10/news.html>>

Lo scorso mese ho scritto: “Una recensione articolata ed interessante di Windows XP SP2, che comprende un elenco di opportunità mancate che avrebbero aumentato la sicurezza. Una lettura consigliata:

<http://www.theregister.co.uk/2004/09/02/winxpsp2_security_review/>”.

Assicuratevi di leggere anche il seguito:

<http://www.theregister.co.uk/2004/09/14/reg_readers_windows/>

L'autore del worm Sasser è stato arrestato...

<<http://www.computerworld.com/printthis/2004/0,4814,95787,00.html>>

<http://www.theregister.co.uk/2004/09/08/sasser_charges/print.html>

...e gli è stato offerto un lavoro:

<<http://australianit.news.com.au/common/print/0,7208,10819809%5E15331%5E%5Enbv%5E15306%2D15318,00.html>> oppure <<http://makeashorterlink.com/?M27156989>>

Uno studio interessante sulla psicologia degli allarmi terroristici:

<<http://www.zimbardo.com/downloads/2002%20Political%20Psychology%20of%20Terrorist%20Alarms.pdf>> oppure <<http://makeashorterlink.com/?Q2A712738>>

Un client e-mail con crittografia per il Treo:

<<http://discussion.treocentral.com/showthread.php?t=57658>>

Lo Honeynet Project sta pubblicando un CD-ROM biennale e una newsletter. Se vi occupate di honeynet, vale davvero la pena di prenderlo e anche se non ve ne occupate, val la pena di supportare questo sforzo.

<<http://www.honeynet.org/funds/cdrom.html>>

CIO Magazine ha pubblicato un sondaggio sulla sicurezza delle informazioni aziendali. Avrei qualcosa da ridire su questo sondaggio, ma ne consiglio comunque la lettura.

<<http://www.itsecurity.com/tecsnews/sep2004/sep143.htm>>

All'Illinois State Capitol, qualcuno ha sparato a una guardia non armata ed è fuggito. Dopo questo incidente, la nuova contromisura di sicurezza adottata è -- tenetevi forte -- cambiare il metodo di ammissione all'interno dell'edificio, passando da una procedura di controllo di badge identificativi, a una procedura che contempla la firma su un registro. Anzitutto, il controllo dell'identità non aumenta la sicurezza. In secondo luogo, perché pensano che un aggressore sia disposto a falsificare/rubare un badge, ma non sia disposto a firmare su un registro?

<<http://www.guardian.co.uk/worldlatest/story/0,1280,-4502926,00.html>>

Un'ottima ricerca: una rete TCP/IP a crittografia quantizzata:

<<http://www.metrowestdailynews.com/localRegional/view.bg?articleid=77990>>

<<http://science.slashdot.org/article.pl?sid=04/09/15/1731216>>

NEC ha i propri risultati di ricerca sulla crittografia quantizzata:

<http://www.infoworld.com/article/04/09/16/HNnecrcryptography_1.html>

Una storia di sicurezza che riguarda l'ambasciata americana in Nuova Zelanda. È un'ottima lezione sulle insidie del non pensare al di là del problema immediato.

<<http://www.stuff.co.nz/stuff/dominionpost/0,2106,3033986a6000,00.html>>

Il futuro dei worm:

<<http://www.computerworld.com/securitytopics/security/story/0,10801,95898,00.html>> oppure

<<http://makeashorterlink.com/?Z38152989>>

Un insegnante è stato arrestato perché il suo segnalibro è stato considerato arma dissimulata:

<http://wjz.com/localstories/local_story_261133455.html>

Vi ricordate di tutte quelle cose che potete portare su un aereo e che possono tramortire le persone? Borsette, computer portatili, libri in edizione rilegata. Anche il filo interdentale, che può essere usato come un cappio, e... e... beh, avete presente.

Pare che sia possibile aprire le serrature Kryptonite per bicicletta usando il cappuccio di una normale biro di plastica. L'attacco funziona secondo quel che i fabbri chiamano il principio dell'"impronta" (impressioning). Le serrature tubolari sono particolarmente vulnerabili perché tutti i perni sono esposti e quegli strumenti che richiedono poca destrezza nell'uso possono essere relativamente semplici. Vi sono stati in commercio per molto tempo alcuni prodotti per fabbri per fare questo ai danni di serrature circolari. Una volta capito il modo di agire, è abbastanza facile farlo. Trovo particolarmente

divertente la soluzione proposta da Kryptonite: adottare un diametro inferiore per la serratura in modo che una certa marca di penne non possa funzionare.

<<http://www.indystar.com/articles/0/179342-1470-223.html>>

<<http://www.wired.com/news/culture/0,1284,64987,00.html>>

<<http://www.bikeforums.net/>>

Spesso mi capita di sostenere come la maggior parte dei firewall non siano efficaci perché non vengono configurati in maniera appropriata. Ecco qualche ricerca sulla configurazione di un firewall:

<<http://www.eng.tau.ac.il/~yash/computer2004.pdf>>

Leggere tag RFID da circa un metro di distanza:

<<http://www.computerworld.com/printthis/2004/0,4814,96051,00.html>>

AOL sta offrendo servizi di autenticazione two-factor. Non sono gratuiti, costano 10 + 2 dollari al mese. Si tratta di un token di sicurezza RSA, con un numero che cambia ogni 60 secondi.

<<http://www.pcworld.com/news/article/0,aid,117873,00.asp>>

Il contro-terrorismo ha il proprio "snake oil":

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

Grandi momenti per i controlli di sicurezza:

<<http://images.ucomics.com/comics/nq/2004/nq041005.gif>>

Il capo della cyber-sicurezza del Governo degli Stati Uniti si è dimesso con un giorno di preavviso. Posso comprendere la sua frustrazione; la sua posizione non aveva più potere, ed era in grado solo di formulare suggerimenti, implorare, e appoggiare una linea di condotta.

<<http://www.computerworld.com/managementtopics/management/story/0,10801,96369,00.html>>

oppure <<http://makeashorterlink.com/?A29135989>>

<<http://www.washingtonpost.com/ac2/wp-dyn/A64915-2004Oct1>> oppure

<<http://makeashorterlink.com/?Q4B122989>>

<<http://www.fcw.com/fcw/articles/2004/0927/web-amit-10-01-04.asp>>

<http://news.com.com/2102-7348_3-5392501.html>

La Corea del Nord aveva più di 500 "cyber-guerrieri" addestrati, secondo il Ministero della Difesa della Corea del Sud. Forse è vero, forse è solo propaganda, da parte del Nord come del Sud. Anche se certamente un qualsiasi militare intelligente addestrerà delle persone nell'arte di attaccare le reti informatiche nemiche.

<http://www.channelnewsasia.com/stories/afp_asiapacific/print/109911/1/.html>

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

Le News di Counterpane

Counterpane ha appena completato un trimestre da record:

<<http://www.counterpane.com/pr-20041014.html>>

Intervista in due parti a Bruce Schneier su SearchSecurity.com:

<http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1011474,00.html>

oppure <<http://makeashorterlink.com/?T1C152989>>

<http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1011476,00.html>

oppure <<http://makeashorterlink.com/?A1D142989>>

Schneier interverrà in tutte le conferenze e gli eventi seguenti:

CSI Asia, a Singapore, il 20 ottobre.

La forza di un algoritmo si basa su due cose: sulla qualità della matematica e su quanto lunga è la chiave. Un sistema sicuro per spezzare un algoritmo è di provare ogni chiave possibile. Gli algoritmi moderni hanno una chiave così lunga che rende impossibile tutto questo; anche se venisse costruito un computer con tutti gli atomi di silicene del pianeta e venisse fatto funzionare per milioni di anni, non sarebbe possibile. Perciò i crittografi cercano delle scorciatoie. Se la matematica che sta dietro all'algoritmo è debole, allora forse esiste un modo per trovare la chiave più velocemente: "spezzare" l'algoritmo.

I cambiamenti apportati dalla NSA causarono scalpore fra i pochi interessati, sia per la "mano invisibile" della NSA (le modifiche non furono rese pubbliche, e non fu pubblicata nessuna analisi ragionata che spiegasse la progettazione finale), sia per la ridotta lunghezza della chiave.

Ma insieme allo scalpore vi fu anche ricerca. Non è un'esagerazione affermare che la pubblicazione di DES creò la moderna disciplina accademica della crittografia. I primi crittografi accademici iniziarono la loro carriera tentando di spezzare DES, o almeno cercando di capire le modifiche apportate dalla NSA. Quasi tutti gli algoritmi crittografici, e la crittografia a chiave pubblica in particolare, possono far risalire le loro radici fino al DES. Studi che analizzano diversi aspetti di DES vengono tuttora pubblicati.

Verso la metà degli anni Novanta si credeva ormai che la NSA fosse in grado di spezzare DES provando ogni chiave possibile. Tale capacità fu dimostrata nel 1998, quando fu costruita una macchina da 220.000 dollari in grado di spezzare a forza bruta una chiave DES in pochi giorni. Nel 1985, la comunità accademica propose una variante a DES, con la stessa matematica ma con una chiave più lunga, chiamata triple-DES. Questa variante è stata utilizzata per anni al posto di DES in applicazioni più sicure, ma era venuto il momento per un nuovo standard. Nel 1997 il NIST sollecitò un algoritmo che rimpiazzasse DES.

Il processo illustra la trasformazione completa della crittografia, da tecnologia segreta della NSA a tecnologia di dominio pubblico a livello mondiale. Il NIST ancora una volta sollecitò l'invio di algoritmi da parte del pubblico, ma in quell'occasione l'agenzia ricevette 15 proposte da 10 diversi paesi. Il mio algoritmo, Twofish, era una di quelle proposte. Dopo due anni di analisi e dibattiti, NIST scelse un algoritmo belga, Rijndael, per creare l'Advanced Encryption Standard (AES).

L'universo della crittografia oggi è molto diverso da quello di 30 anni fa. Sappiamo molte più cose sulla crittografia, e abbiamo più algoritmi fra cui scegliere. AES non diventerà uno standard così largamente diffuso come fu DES a suo tempo. Ma si sta facendo strada in prodotti di sicurezza per le banche, nei protocolli di sicurezza in Internet, e persino nelle macchine per il voto elettronico. Uno standard NIST è un imprimatur di qualità e sicurezza, e i produttori lo riconoscono.

Insomma, quanto è in gamba la NSA in fatto di crittografia? Sicuramente è migliore del mondo accademico. Possiede un maggior numero di matematici che lavorano sui problemi, ci hanno lavorato più a lungo, ed hanno accesso a tutto quanto è stato pubblicato nel mondo accademico e dal canto loro non devono rendere pubblici i loro risultati. Ma quanto sono avanti rispetto allo stato dell'arte? Un anno? Cinque anni? Dieci? Nessuno lo sa.

La comunità accademica ha impiegato vent'anni per capire che le "modifiche" della NSA miglioravano effettivamente la sicurezza di DES. Questo vuol dire che negli anni Settanta, la National Security Agency era 20 anni avanti rispetto allo stato dell'arte.

Oggi la NSA è ancora avanti, ma il resto della comunità sta riducendo il divario piuttosto rapidamente. Nel 1999, la comunità accademica ha scoperto una vulnerabilità in un altro algoritmo della NSA, SHA, algoritmo che la NSA aveva dichiarato di aver scoperto solo quattro anni prima. Solo la settimana scorsa è stata pubblicata un'analisi dell'algoritmo SHA-1 che dimostra alcune vulnerabilità che crediamo la NSA non conoscesse nemmeno.

Forse oggi siamo solo un paio d'anni indietro.

La sorveglianza all'ingrosso sta diventando rapidamente la norma. Lo E-Z Pass di New York tiene traccia delle auto che si trovano in prossimità di tunnel e ponti con pedaggio. Tutti possiamo essere tracciati attraverso i nostri telefonini. I nostri acquisti vengono tracciati dalle banche e dalle compagnie di carte di credito. Le nostre abitudini di navigatori Internet sono tracciate da chi opera nei siti Web. Telecamere di sicurezza si trovano ovunque. Se volesse, la polizia potrebbe prendere il database di veicoli equipaggiati con il sistema di tracciamento OnStar, e localizzare immediatamente tutte le auto a New Haven.

Come gli scanner di targhe automobilistiche, le impronte digitali elettroniche che lasciamo dappertutto possono essere automaticamente correlate a dei database. I dati possono venire registrati permanentemente, dando così alla polizia la possibilità di condurre la sorveglianza indietro nel tempo.

Gli effetti della sorveglianza all'ingrosso sulla privacy e sulle libertà civili è profonda; purtroppo, però, il dibattito viene spesso male interpretato e reso nei termini di quanta privacy dobbiamo abbandonare per essere sicuri. Questo è sbagliato. È ovvio che si è tutti più sicuri quando la polizia può sfruttare ogni genere di tecnica che possiede. Ciò di cui abbiamo bisogno sono dei meccanismi corrispondenti per prevenire gli abusi, e che non costituiscano un fardello inaudito per gli innocenti.

Attraverso l'intera storia del nostro paese, abbiamo mantenuto un equilibrio fra gli interessi necessari della polizia e i diritti civili della gente. La stessa targa automobilistica rappresenta un simile equilibrio. Immaginate il dibattito nei primi anni del Novecento: la polizia propone di affiggere sui ogni veicolo una targa con il nome del proprietario, in modo da poter meglio tracciare le auto usate per compiere reati. I difensori delle libertà civili sono contrari, perché questo avrebbe diminuito la privacy dei possessori del veicolo. Allora viene raggiunto un compromesso: una stringa casuale di lettere e numeri che la polizia poteva usare per risalire al proprietario del veicolo. Ideando volontariamente un sistema più burocratizzato, le esigenze delle forze dell'ordine e il diritto alla privacy delle persone venivano bilanciati.

Un altro sistema di bilanciamento è il processo per l'ottenimento di un mandato di perquisizione, come descritto nel Quarto Emendamento. E allo stesso modo funziona il requisito di minimizzazione contemplato nelle intercettazioni telefoniche: la polizia deve smettere di stare in ascolto su una linea telefonica se il sospetto che viene indagato non sta parlando.

Per difendersi dagli scanner di targhe automobilistiche, una protezione piuttosto ovvia sarebbe quella di richiedere che la polizia cancelli subito i dati raccolti su innocenti proprietari di auto, senza registrarli. La polizia non ha alcun bisogno legittimo di raccogliere dati sulle abitudini di guida di tutti. Un altro modo di proteggersi è quello di permettere ai possessori di un veicolo di accedere alle informazioni raccolte su di loro durante una di queste ricerche automatizzate, e di permettere loro di fare ricorso in caso di errori.

Ma dobbiamo spingerci oltre. Le sanzioni penali sono severe in modo da creare un deterrente, dato che è difficile acciuffare i delinquenti. Nel momento in cui diventa più semplice acciuffarli, occorre effettuare un riallineamento. Quando la polizia sarà in grado di automatizzare la rilevazione di un reato, forse si potrebbe evitare di comminare sanzioni penali. Ad esempio, le telecamere che rilevano infrazioni come passare col rosso o superare i limiti di velocità potrebbero emettere delle citazioni senza perdita di "punti" ai danni del guidatore.

La sorveglianza all'ingrosso non è semplicemente un sistema più efficace che permette alla polizia di fare ciò che ha sempre fatto. È un vero e proprio nuovo potere nelle mani della polizia, un potere reso possibile dalla tecnologia attuale e che sarà sempre più facile esercitare grazie alla tecnologia di domani. E, come con ogni nuovo potere di polizia, noi in quanto società dobbiamo pretendere un ruolo attivo nello stabilire delle regole che ne governino l'uso. Agire diversamente significa cedere un'autorità ancora maggiore alle forze dell'ordine.

Questo articolo è stato originariamente pubblicato nel New Haven Register.

<http://www.nhregister.com/site/news.cfm?newsid=12954895&BRD=1281&PAG=461&dept_id=517515&rfti=8> oppure <<http://makeashorterlink.com/?K2F132989>>

** **

Sorveglianza aerea per rilevare violazioni nel codice di costruzione

<http://www.schneier.com/blog/archives/2004/10/aerial_surveill.html>

In maniera simile a quanto visto nell'articolo precedente, la città di Baltimore sta utilizzando materiale fotografico prodotto dalla sorveglianza aerea per rilevare violazioni nel codice di costruzione degli edifici. Ho scritto un editoriale di opinione per il Baltimore Sun a riguardo, usando più o meno gli stessi concetti sopra riportati.

<<http://www.baltimoresun.com/news/opinion/oped/bal-op.spying04oct04,1,7874969.story>> or <<http://makeashorterlink.com/?O20221989>>

** **

Allarmi di minaccia terroristica

Ho scritto due articoli sugli allarmi di minaccia terroristica, e su quanto siano inutili come misure di sicurezza.

L'articolo sul Minneapolis Star-Tribune:

<<http://www.schneier.com/essay-055.html>>

L'articolo su Rake:

<http://www.schneier.com/blog/archives/2004/10/do_terror_alert.html>

** **

La libertà accademica e la sicurezza

<http://www.schneier.com/blog/archives/2004/10/academic_freedo.html>

La crittografia è la scienza dei codici segreti, ed è uno strumento primario della sicurezza in Internet per combattere hacker, il crimine e il terrorismo cibernetico. CRYPTO è la conferenza sulla crittografia più importante nel mondo. Viene tenuta ogni mese di agosto a Santa Barbara.

Quest'anno, 400 persone provenienti da 30 paesi sono venute per ascoltare decine di tavole rotonde e di discussioni. Lu Yi non ha potuto intervenire. Il suo studio è stato accettato alla conferenza, ma dato che lei è una studentessa ricercatrice cinese in Svizzera, non ha avuto la possibilità di ottenere in tempo il visto per poter partecipare alla conferenza.

Nei tre anni successivi alla tragedia dell'11 settembre, il governo degli Stati Uniti ha istituito una serie di misure di sicurezza alle nostre frontiere, tutte pensate per tenere a distanza i terroristi. Una di queste misure è stata quella di rendere più severa la regolamentazione per i visti stranieri. Questo ha certamente colpito l'industria del turismo negli USA, ma il danno provocato alla ricerca accademica è più profondo e durevole.

comportino altre marche, ma credo che vi sia un simile meccanismo). Era persino scritto nel manuale utente del mio vecchio Nokia 3110, se ricordo bene. Credo che si faccia così perché i numeri di telefono possono essere memorizzati in forma nazionale o internazionale dall'utente stesso, ed anche l'identificativo chiamante (caller ID) può essere diverso da operatore a operatore. Ad esempio Bouygtel, in Francia, visualizza i numeri in formato internazionale, mentre SFR utilizza il formato nazionale a 10 cifre (che inizia per 0). SFR ha scelto quel formato di visualizzazione dell'identificativo chiamante probabilmente perché lo ritiene più semplice da memorizzare da parte degli utenti.

Sette cifre, con ogni probabilità, sarà sembrato un buon compromesso, dato che è una serie sufficientemente lunga per mantenere bassa la probabilità di collisione (a meno che non si stia intenzionalmente effettuando uno spoofing dell'identificativo chiamante) e sufficientemente corta per non tenere conto di un eventuale prefisso variabile...

Non ci ho mai pensato, ma questa potrebbe essere una valida ragione affinché gli operatori non diano alle persone la facoltà di scegliersi il numero. Anche se non è più il caso, alcuni anni fa Bouygtel permetteva di scegliere le ultime 4 cifre del numero di telefono, come incentivo commerciale.

Da: "Howze, Blair" <BHowze@co.gallatin.mt.us>
Oggetto: La sicurezza alle Olimpiadi

Esiste un certo valore intrinseco nel "mostrare il badge" a cui lei non ha dato molto credito. Dobbiamo preoccuparci anche dei comuni delinquenti, e pare che la massiccia presenza di personale munito di badge abbia avuto una certa efficacia nel far diminuire il numero di incidenti.

Che il risultato sia valso la cifra spesa, possiamo discuterne. Anche se i badge non sono il solo deterrente credibile per dei terroristi suicidi, fa in modo che il potenziale terrorista pianifichi l'azione evitando gli "occhi aggiunti" dell'aumentata forza di sicurezza.

In secondo luogo, nella maggior parte dei casi la sicurezza è stata probabilmente disposta sapendo che non sarebbe stata in grado di fermare un individuo determinato, intelligente, suicida (o comunque qualcuno a cui non importasse nulla delle conseguenze). I servizi segreti statunitensi sono molto preoccupati da questo tipo di attacco perché le operazioni di intelligence hanno diminuito la loro efficacia contro chi agisce in solitario e sa mantenere un segreto. Perciò spendono la maggior parte delle energie e del denaro fermando attacchi coordinati, dove il numero di individui coinvolti fa aumentare la probabilità che qualche informazione salti fuori.

Sono d'accordo che si raggiunge il punto dei rendimenti decrescenti. Purtroppo, il pubblico americano (e per un certo grado, il mondo occidentale) sembra intento a classificare ogni singolo decesso a opera di terroristi come un fallimento dell'intero sistema di intelligence, delle operazioni militari, della leadership, ecc.

Perciò, i pubblici ufficiali e il loro staff sono molto più inclini a spendere cifre esorbitanti per prevenire ogni genere di incidente, e per evitare di essere puniti.

Lei ha scritto: "Sarebbe stato molto più efficace spendere molto di quel miliardo e mezzo di dollari in intelligence e in servizi di pronto intervento in caso di emergenze. L'intelligence è uno strumento inestimabile contro il terrorismo, e funziona a prescindere da ciò che i terroristi stanno architettando..."

La sicurezza È STATA EFFICACE alle Olimpiadi. Non c'è stato alcun grave incidente. Sono sicuro che ne sarebbero potuti accadere, ma per tutta una serie di ragioni (delle quali una almeno è la fortuna) non è successo nulla. Tuttavia, il denaro è stato speso solo per una singola occasione, e questo non ha contribuito all'obiettivo generale a lungo termine di ridurre l'efficacia delle organizzazioni terroristiche. Ciò che lei dice in merito allo spendere più del totale sui processi e l'infrastruttura dell'intelligence e della risposta all'emergenza, è azzeccatissimo. Diciamo che tutto si riduce a una

questione di punti di vista. Il punto di vista degli organizzatori della sicurezza delle Olimpiadi è stato egoistico, per il fatto che la loro unica preoccupazione fosse limitata all'evento olimpico. A loro non importa ciò che accadrà l'anno prossimo, perché sarà il problema di qualcun altro. Per cui si sono concentrati sullo spendere il denaro su ciò che poteva essere messo ben in vista. Ha funzionato, tutto sommato. Non sarà stato il piano migliore, ma ha avuto una certa efficacia. Occorre ricordare il gran numero di interessi in ballo nella pianificazione del sistema di sicurezza. Soltanto immaginare gli interessi politici che ci sono dietro fa inorridire.

Da: Anonimo

Oggetto: La paura e la sicurezza

Questo è in risposta alla lettera da lei pubblicata il mese scorso a firma Wayne Schroeder: la paura e la sicurezza viaggiano a braccetto in situazioni semplici, come guidare una motocicletta. Il sistema per ridurre la paura è quello di aumentare la propria sicurezza, ad esempio guidando più lentamente. Milioni di anni di evoluzione hanno fatto evolvere la paura come meccanismo per tenerci in vita, ma milioni di anni di evoluzione non hanno mai avuto a che fare con un 767. Si è evoluto per cose più semplici, come il brutto tempo, le alte velocità e gli animali feroci.

Quando bisogna affrontare le situazioni di sicurezza più complesse del mondo moderno, i nostri istinti naturali sono inadeguati. Però le persone continuano a farsi guidare da essi, come nell'ormai famigerato episodio di Annie Jacobsen. Ecco perché esiste il "teatrino" della sicurezza: la gente sta cercando di ridurre la paura, non di aumentare la sicurezza, e non si rende conto che queste cose non sono più le stesse di una volta.

Questo spiega anche il perché le persone siano riluttanti a confrontare le loro scelte mediocri. Quando le obblighi a farlo, le porti da una situazione di paura lieve ad una di paura maggiore; e per quanto ne sanno, sei tu a causare la paura. Da un punto di vista razionale, è chiaro che le stai rendendo più sicure, ma loro non la vedono così.

L'esempio della motocicletta non regge perché si rapporta facilmente ai nostri istinti evoluti. I moderni problemi di sicurezza sono così complicati che i modi per ridurre la paura si sono divisi da quelli per aumentare l'incolumità. Cercare di rapportare queste emozioni primitive a minacce odierne non può funzionare, il divario è troppo grande. Affidarsi alle nostre paure perché ci guidino nelle nostre scelte non ci renderà più sicuri: renderà il tutto ancora più scioccante quando le nostre difese verranno abbattute ancora una volta.

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

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.

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) 2004 by Bruce Schneier.