

CRYPTO-GRAM
15 agosto 2009

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

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

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

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

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

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

Crypto-Gram è anche consultabile in formato RSS.

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

In questo numero:

- L'intuizione dei rischi
- La prominenza della privacy e i siti di social networking
- Incorporare la sorveglianza
- News
- La sicurezza dei portatili alle frontiere
- Protocolli self-enforcing
- Le news su Schneier
- Un altro nuovo attacco contro AES
- Lo scassinamento delle serrature e Internet
- Commenti dei lettori

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

L'intuizione dei rischi

Le persone hanno un'intuizione naturale per i rischi, e per molti versi è assai buona. A volte è inefficace a causa di una serie di bias cognitivi, ma per quei rischi normali che si incontrano regolarmente, essa funziona sorprendentemente bene; spesso meglio di quanto siamo disposti a riconoscerlo. Per questo sono rimasto sorpreso mentre ascoltavo l'ennesimo moderatore di una conferenza lamentarsi dell'addestramento alla sicurezza. Stava parlando della difficoltà di fare in modo che i dipendenti della sua

azienda seguissero davvero le sue politiche di sicurezza: criptare i dati su memory stick, non condividere le password, non effettuare il login da reti wireless non fidate. "Dobbiamo far sì che le persone comprendano i rischi", ha detto.

A me sembra che i suoi colleghi abbiano una comprensione dei rischi migliore della sua. Loro sanno quali siano i veri rischi in gioco, e che tutti ruotano intorno al non compiere il proprio lavoro. Quei rischi sono reali e tangibili, e i dipendenti li provano in continuazione. I rischi legati al non seguire le procedure di sicurezza sono molto meno reali. Magari un impiegato verrà beccato, ma probabilmente no. E anche se viene beccato, le sanzioni non sono così gravi.

Data questa precisa analisi dei rischi, ogni dipendente dotato di razionalità aggirerà costantemente la sicurezza allo scopo di portare a termine il proprio lavoro. Questo è ciò che l'azienda premia, e ciò che l'azienda vuole davvero.

"Licenzi chiunque non segua le procedure di sicurezza, rapidamente e pubblicamente", ho suggerito a quel moderatore. "Questo farà aumentare l'attenzione per la sicurezza molto più in fretta di tutti i suoi poster, discorsi o newsletter". Se i rischi sono reali, le persone li comprenderanno.

È possibile osservare lo stesso genere di intuizione dei rischi sulle autostrade. Si presta meno attenzione ai limiti di velocità dichiarati che non ai limiti veri e propri, quelli per cui si può essere multati dalla polizia. Stesso discorso sulle strade: la gente reagisce ai tassi di criminalità veri e propri, non ai pubblici funzionari che dichiarano che un certo quartiere è sicuro.

Gli avvisi scritti sugli adesivi applicati alle scale a pioli potrebbero far pensare che le scale siano di gran lunga più rischiose di quanto lo siano in realtà, ma le persone hanno una buona intuizione per quanto riguarda l'uso di questi oggetti, e ignorano la maggioranza degli avvisi. (Ciò non vuol dire che alcune persone non facciano stupidaggini con le scale, ma nella maggior parte dei casi sono al sicuro. Gli avvisi servono soprattutto a mitigare i rischi di eventuali cause legali per i fabbricanti di scale, e non riguardano tanto i rischi per chi vi si arrampica).

In quanto specie, siamo per natura sintonizzati sui rischi inerenti al nostro ambiente. Attraverso l'evoluzione, la nostra sopravvivenza è dipesa dal prendere intuitivamente decisioni di gestione dei rischi ragionevolmente precise, e siamo talmente bravi a farlo che non ce ne accorgiamo nemmeno.

I genitori lo sanno bene. I bambini sono dotati di una intuizione dei rischi sorprendentemente perspicace. Sanno quando i genitori fanno sul serio e quando le loro minacce sono inconsistenti. E rispondono ai rischi reali di un'eventuale punizione da parte dei genitori, non ai rischi ingigantiti basati sulla retorica degli adulti. Ancora una volta, non serviranno lezioni sull'addestramento all'attenzione; devono esserci conseguenze reali, tangibili.

E il tutto si fa ancora più strano. John Adams, professore all'University College London ha reso popolare la metafora del 'termostato di rischio' mentale. Tendiamo a ricercare un certo livello naturale di rischio, e se qualcosa diventa meno rischioso, abbiamo la tendenza a renderlo più rischioso. I motociclisti con il casco vanno più forte di quelli senza casco.

I nostri termostati di rischio non sono perfetti (quel motociclista con casco avrà comunque mitigato i suoi rischi) e tendono a rimanere nello stesso campo (andrà anche più forte, ma non aumenterà i suoi rischi iniziando a fumare) ma, in generale, le persone dimostrano una capacità innata e ben regolata di comprendere e rispondere ai rischi.

Naturalmente la nostra intuizione dei rischi fallisce spesso e miseramente nel caso di rischi rari, sconosciuti, volontari, eccetera. Ma quando si confronta con i rischi comuni che affrontiamo quotidianamente (quei generi di rischi da cui è dipesa la nostra sopravvivenza evolutiva) ce la caviamo molto bene.

Per cui, ogni volta che vedete qualcuno in una situazione e pensate che questa persona non ne comprende i rischi, fermatevi e assicuratevi di aver capito voi, in primis, tali rischi. Potreste avere delle sorprese.

Questo articolo è apparso in precedenza sul Guardian.

<<http://www.guardian.co.uk/technology/2009/aug/05/bruce-schneier-risk-security>>
oppure <<http://tinyurl.com/ngu224>>

Il termostato del rischio:

<http://www.amazon.com/Risk-John-Adams/dp/1857280687/ref=sr_1_1?ie=UTF8∓sr=8-1>

oppure <<http://tinyurl.com/kwmuz9>>
<<http://davi.poetry.org/blog/?p=4492>>

Fallimenti nell'intuizione dei rischi:

<<http://www.schneier.com/essay-155.html>>
<<http://www.schneier.com/essay-171.html>>

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

La prominenza della privacy e i siti di social networking

Rassicurare le persone in merito alla privacy le preoccupa di più, e non di meno. Viene chiamata "privacy salience" (prominenza, importanza della privacy) e Leslie John, Alessandro Acquisti e George Loewenstein (tutti della Carnegie Mellon University) lo hanno dimostrato in una serie di brillanti esperimenti. In uno di questi i soggetti hanno completato un sondaggio online che consisteva in una serie di domande inerenti il loro comportamento accademico: "Avete mai barato a un esame?", per esempio. A metà del gruppo dei soggetti è stato richiesto di firmare un consenso, ideato per rendere le questioni di privacy maggiormente prominenti, mentre all'altra metà del gruppo non è stato presentato alcun consenso. Inoltre a una serie di soggetti scelti a caso veniva inviata una promessa formale sulla confidenzialità della privacy. Quando al tema della privacy veniva data prominenza (attraverso il consenso da firmare), le persone reagivano negativamente alla seguente rassicurazione della natura confidenziale del test, e tendevano a non rivelare informazioni personali.

In un altro esperimento, i soggetti hanno completato un sondaggio online in cui venivano presentate loro diverse domande di natura personale, come "Avete mai

provato la cocaina?”. A metà del gruppo dei soggetti è stato presentato un sondaggio dai toni frivoli (“Quanto siete cattivi?”) con l’immagine di un diavoletto simpatico. L’altra metà del gruppo ha completato lo stesso sondaggio, intitolato però “Sondaggio della Carnegie Mellon University sugli standard etici”, con tanto di sigillo universitario e assicurazioni ufficiali sulla privacy. I risultati hanno dimostrato che le persone a cui si era ricordata la questione della privacy erano meno propense a rivelare informazioni personali rispetto agli altri soggetti.

La prominenza della privacy serve in gran parte a spiegare i meccanismi e gli atteggiamenti dei siti di social networking nei confronti della privacy. Da un punto di vista commerciale, i siti di social networking non vogliono che i propri membri si preoccupino di esercitare i loro diritti di privacy. Preferiscono che i membri si sentano a proprio agio nel rivelare molto di sé.

Joseph Bonneau e Soeren Preibusch della Cambridge University hanno studiato la privacy in 45 siti di social networking popolari in tutto il mondo (forse nemmeno sapevate che esistono 45 siti di social networking popolari in tutto il mondo). Hanno scoperto che le impostazioni di privacy erano spesso complicate e difficili da accedere; Facebook, con le sue 61 impostazioni di privacy, è il peggiore sotto questo punto di vista. Per comprendere alcuni dei settaggi, hanno dovuto creare account con regolazioni differenti per poter confrontare i risultati. La privacy tende ad aumentare con l’età e la popolarità di un sito. Siti di uso generale tendono ad avere più funzionalità legate alla privacy rispetto a siti di nicchia.

Ma la scoperta più interessante di Bonneau e Preibusch è che i siti nascondono regolarmente ogni riferimento alla privacy. Le loro pagine introduttive parlano di connettersi con gli amici, di incontrare nuove persone, di condividere foto: i vantaggi del rivelare dati personali.

Questi siti parlano anche di privacy, naturalmente, ma soltanto su pagine di policy sulla privacy molto difficili da trovare. Qui i vari siti forniscono forti rassicurazioni in merito ai propri controlli sulla privacy e alla sicurezza dei dati che i membri decidono di rivelare sui siti. Vengono visualizzati stemmi di entità di privacy di terze parti e altre simili icone atte a calmare eventuali paure che i membri possano avere in questo senso.

È il risultato sperimentale della Carnegie Mellon nel mondo reale. Agli utenti interessa la privacy, ma non è che vi pensano in continuazione ogni giorno. I siti di social networking non vogliono ricordare la privacy agli utenti, anche se ne parlano in maniera positiva, perché ogni menzione di essa farà in modo di ricordare agli utenti le loro paure legate alla privacy dei dati, rendendoli più cauti e guardinghi sulla condivisione delle informazioni personali. Tuttavia i siti devono anche assicurare tutti quei “fondamentalisti della privacy” per i quali la privacy è sempre importante e prominente, pertanto preparano una retorica pro-privacy molto forte per chi ha tempo di cercare informazioni sulle policy di privacy di questi siti. I due diversi messaggi di marketing sono indirizzati a due pubblici diversi.

I siti di social networking stanno migliorando le proprie impostazioni di privacy a seguito della pressione del pubblico. Allo stesso tempo esiste una opposta pressione commerciale che spinge verso una diminuzione della privacy; osservate ciò che sta accadendo adesso su Facebook, per esempio. Ingenuamente, dovremmo aspettarci che le compagnie rendano il più possibile chiare le proprie policy di privacy per consentire ai clienti di compiere una scelta informata. Ma il bisogno di marketing di ridurre la

prominenza della privacy ostacolerà eventuali soluzioni di mercato per migliorare la privacy; i siti preferiscono di gran lunga offuscare la questione piuttosto che competere con essa come funzione.

Questo articolo è originariamente apparso sul Guardian.

<<http://www.guardian.co.uk/technology/2009/jul/15/privacy-internet-facebook>>
oppure <<http://tinyurl.com/ml7kv4>>

Esperimenti di privacy:

<http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1430482>

La privacy e i siti di social networking:

<http://www.cl.cam.ac.uk/~jcb82/doc/privacy_jungle_bonneau_preibusch.pdf>

Facebook:

<<http://www.insidefacebook.com/2009/05/13/facebook-privacy-guide/>>

<<http://www.nytimes.com/external/readwriteweb/2009/06/24/24readwriteweb-the-day-facebook-changed-messages-to-become-18772.html>>

oppure <<http://tinyurl.com/lqpfh8>>

<<http://www.allfacebook.com/2009/02/facebook-privacy>>

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

Incorporare la sorveglianza

La Cina è il miglior censore di Internet del mondo. Malgrado il 'Grande Firewall cinese' non sia perfetto, riesce efficacemente a limitare il flusso di informazioni in entrata e in uscita dal paese. Ora però il governo cinese sta portando le cose un passo oltre.

Secondo un provvedimento che entrerà in vigore molto presto, ogni computer venduto in Cina dovrà contenere un pacchetto software chiamato Green Dam Youth Escort. Un filtro per la pornografia, in apparenza, ma in realtà si tratta di spyware governativo che terrà d'occhio ogni cittadino su Internet.

Green Dam si presta a molti usi. Può sorvegliare una serie di siti Web proibiti. Può controllare le abitudini di lettura di un utente. Può persino far partecipare un computer in un gigantesco attacco botnet, come parte di un'ipotetica guerra cibernetica.

Le azioni della Cina possono sembrare estreme, ma non sono eccezionali o uniche. Altri governi democratici nel mondo (Svezia, Canada e Regno Unito, per esempio) stanno cercando di far passare in tutta fretta una serie di leggi che diano alle proprie forze di polizia nuovi poteri di sorveglianza telematica, in molti casi richiedendo ai provider di sistemi di comunicazione di ridisegnare i prodotti e i servizi che vendono.

Molti stanno passando leggi sulla conservazione dei dati, obbligando le aziende a conservare informazioni sui loro clienti. Proprio di recente, il governo tedesco ha proposto di riservarsi il potere di censurare Internet.

Gli Stati Uniti non fanno eccezione. La legge CALEA del 1994 richiedeva alle compagnie telefoniche di facilitare le intercettazioni dell'FBI, e dal 2001 la NSA ha costruito sistemi

di intercettazione significativi all'interno degli Stati Uniti. Il governo ha ripetutamente proposto leggi per la conservazione dei dati Internet, permettendo la sorveglianza su attività passate e presenti.

Sistemi come questo sono un invito aperto all'appropriazione criminale e all'abuso da parte del governo stesso. Nuovi poteri di polizia, instaurati per combattere il terrorismo, vengono già impiegati in situazioni di reati comuni. Il controllo e la sorveglianza su Internet non saranno diversi.

Gli abusi ufficiali sono già nocivi di per sé, ma sono gli usi non ufficiali che mi preoccupano di più. Un qualsiasi sistema di sorveglianza e controllo deve essere protetto e sicuro a sua volta. Una infrastruttura che favorisce la sorveglianza e il controllo invita alla sorveglianza e al controllo, sia da parte di persone che ci si aspetta, sia da parte di chi non ci si aspetta.

Il governo cinese ha ideato Green Dam per i propri scopi e utilizzi, ma è stato sovvertito. Perché si pensa che i criminali non saranno in grado di servirsene per sottrarre informazioni su conti bancari e carte di credito, per lanciare altri attacchi, o per convertirlo in un enorme botnet per inviare spam?

Perché si pensa che soltanto membri autorizzati delle forze dell'ordine raccoglieranno e gestiranno i dati telematici o effettueranno intercettazioni telefoniche e/o di messaggia istantanea?

Questi rischi non sono affatto teorici. Dopo l'11 settembre, la National Security Agency ha costruito un'infrastruttura di sorveglianza per intercettare telefonate ed email all'interno degli Stati Uniti.

Malgrado le regole procedurali avessero stabilito che si sarebbero dovute intercettare soltanto le chiamate di cittadini non americani e le chiamate internazionali, nella pratica non sempre si sono rispettate tali regole. Gli analisti della NSA hanno raccolto molte più informazioni di quanto fossero autorizzati, e si sono serviti del sistema per spiare mogli, fidanzate e personaggi famosi come l'ex presidente Clinton.

Ma questo non è l'uso improprio più grave di un'infrastruttura di sorveglianza delle telecomunicazioni. In Grecia, fra il giugno 2004 e il marzo 2005, qualcuno ha tenuto sotto controllo più di cento telefoni cellulari appartenenti a membri del governo greco: il primo ministro e i ministri della difesa, degli esteri e della giustizia.

Ericsson aveva inserito questa possibilità di intercettazione nei prodotti Vodafone, e l'aveva abilitata solamente per quei governi che ne avevano fatto richiesta. La Grecia non era uno di quei governi, ma qualcuno ancora ignoto (un partito politico rivale? Il crimine organizzato?) ha scoperto come attivare quella funzione segretamente.

I ricercatori hanno già scoperto delle falle di sicurezza in Green Dam che potrebbero permettere a degli hacker di prendere possesso dei computer. Naturalmente vi sono altre vulnerabilità, e i criminali le stanno cercando.

L'infrastruttura di sorveglianza può essere esportata, il che incentiva il totalitarismo nel mondo. Compagnie occidentali come Siemens, Nokia e Secure Computing hanno costruito l'infrastruttura di sorveglianza dell'Iran. Aziende statunitensi hanno contribuito

alla realizzazione dello stato di polizia elettronico cinese. L'anonimato di Twitter ha salvato le vite dei dissidenti iraniani; anonimato che molti governi vogliono eliminare.

Ogni anno porta con sé un controllo e una censura di Internet sempre maggiori, e non solo in paesi come la Cina e l'Iran, ma anche negli Stati Uniti, nel Regno Unito, in Canada e in altri paesi liberi.

Il movimento per il controllo viene istigato sia dalle forze dell'ordine, che vogliono fermare terroristi, pedopornografi e altri criminali, sia dalle aziende di contenuti multimediali, che vogliono fermare chi condivide i file attraverso il peer-to-peer.

È una pessima igiene civica costruire tecnologie che un giorno potrebbero essere utilizzate per facilitare l'istituzione di uno stato di polizia. Non importa quel che dicono intercettatori e censori: questi sistemi espongono tutti noi a rischi ancor più seri. I sistemi di comunicazione che non incorporano funzioni di intercettazione sono più sicuri di sistemi dotati di quelle capacità.

Questo articolo è precedentemente apparso (con un minor numero di rimandi) sul sito della Minnesota Public Radio.

<<http://minnesota.publicradio.org/display/web/2009/07/30/schneier/>>

Una copia di questo articolo, con i rimandi integrati nel testo, è disponibile sul mio blog:

<http://www.schneier.com/blog/archives/2009/08/building_in_sur.html>

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

News

Possono avvenire fughe di dati attraverso le linee elettriche; la NSA lo sa da decenni:

<<http://news.bbc.co.uk/2/hi/technology/8147534.stm>>

Oggi vi è molta ricerca aperta sui side channel.

<http://www.schneier.com/blog/archives/2008/10/remotely_eavesd.html>

<http://www.schneier.com/blog/archives/2009/06/eavesdropping_o_3.html>

<<http://www.schneier.com/paper-side-channel.html>>

Il Sudafrica prende sul serio le questioni di sicurezza. Ecco uno sportello Bancomat che spruzza automaticamente dello spray al peperoncino in faccia a chi "manomette gli slot delle tessere". Non sembra una cattiva idea, ma in questo genere di cose occorre stare attenti all'alto numero di falsi positivi.

<<http://www.guardian.co.uk/world/2009/jul/12/south-africa-cash-machine-pepper-spray>>

oppure <<http://tinyurl.com/nj5zks>>

Uno studio sul crimine cibernetico: "Distributed Security: A New Model of Law Enforcement" (Sicurezza distribuita: un nuovo modello per far rispettare la legge) di Susan W. Brenner e Leo L. Clarke. È del 2005 ma non lo avevo mai visto prima.

<http://papers.ssrn.com/sol3/papers.cfm?abstract_id=845085>

La crittografia può avere prove di non conoscenza (zero knowledge), nel senso che Alice può provare a Bob che conosce qualcosa senza rivelarlo a Bob. Ecco qualcosa di

simile nel mondo reale: un progetto di ricerca per permettere agli ispettori degli armamenti di una nazione di verificare lo stato dello smantellamento di armi nucleari di un'altra nazione senza scoprire alcun segreto durante il procedimento (per esempio quanto materiale nucleare è contenuto nelle armi).

<<http://news.bbc.co.uk/2/hi/europe/8154029.stm>>

Ho già parlato di tracciare schemi sull'uso delle droghe effettuando test sulle acque fognarie, nel 2007. Ora vi sono delle nuove ricerche in merito:

<http://www.schneier.com/blog/archives/2009/07/mapping_drug_us.html>

Eccellente articolo che tratta in dettaglio l'attacco contro Twitter.

<<http://www.techcrunch.com/2009/07/19/the-anatomy-of-the-twitter-attack/>>

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

I numeri di previdenza sociale non sono casuali. In alcuni casi si possono prevedere avendo la data e il luogo di nascita.

<http://www.nhregister.com/articles/2009/07/07/news/a1 -- id_theft.txt>

<<http://redtape.msnbc.com/2009/07/theres-a-new-reason-to-worry-about-the-security-of-your-social-security-number-turns-out-theyre-easy-to-guess--a-gro.html>>

oppure <<http://tinyurl.com/n8o7kf>>

<<http://www.wired.com/wiredscience/2009/07/predictingsasn/>>

<<http://www.cnn.com/2009/US/07/10/social.security.numbers/index.html>>

<<http://www.pnas.org/content/106/27/10975>>

<<http://www.pnas.org/content/early/2009/07/02/0904891106.full.pdf>>

<<http://www.heinz.cmu.edu/~acquisti/ssnstudy/>>

Non vedo nessuna nuova vulnerabilità qui. Già sappiamo che i numeri di previdenza sociale non sono segreti. E chiunque voglia sottrarre un milione di questi numeri è molto più probabile che entri in uno dei tantissimi database esistenti che li conservano.

Il NIST ha annunciato i 14 candidati SHA-3 che sono passati al secondo turno: BLAKE, Blue Midnight Wish, CubeHash, ECHO, Fugue, Grostl, Hamsi, JH, Keccak, Luffa, Shabal, SHAvite-3, SIMD e Skein. A febbraio scelsi i miei preferiti: Arirang, BLAKE, Blue Midnight Wish, ECHO, Grostl, Keccak, LANE, Shabal e Skein. Fra quelli scelti dal NIST sono molto sorpreso di vedere CubeHash e molto sorpreso di non vedere LANE.

<http://csrc.nist.gov/groups/ST/hash/sha-3/Round2/submissions_rnd2.html>

<<http://www.schneier.com/essay-249.html>>

<<http://csrc.nist.gov/groups/ST/hash/sha-3/index.html>>

<<http://www.skein-hash.info/>>

Buona descrizione della 'base rate fallacy' (fallacia della probabilità primaria).

<http://news.bbc.co.uk/2/hi/uk_news/magazine/8153539.stm>

Divertente: "Consigli per rimanere al sicuro online":

<http://www.schneier.com/blog/archives/2009/07/tips_for_stayin.html>

Pare che in Svizzera lo spazio necessario a conservare oro in maniera sicura stia finendo. Se questo è vero, si tratta di un grave problema di sicurezza. Non si può conservare l'oro proteggendolo con normali serrature. Costruire luoghi destinati alla conservazione dell'oro richiede tempo e denaro.

<<http://www.commodityonline.com/news/Swiss-banks-have-no-space-left-for-gold!-19698-3-1.html>>

oppure <<http://tinyurl.com/kqpm8w>>

Mi ricordo di un problema simile, che l'Unione Europea ha avuto durante la transizione all'Euro: dove conservare tutte le banconote e le monete prima del passaggio alla nuova valuta. Nei caveau delle banche non c'era spazio sufficiente, perché la stragrande maggioranza di una moneta è in circolazione. La questione è simile, anche se le banche europee poterono risolvere il problema con un maggior numero di guardie, visto che l'inconveniente era soltanto temporaneo.

Un grosso cartello con la scritta "Stati Uniti" a un passaggio di frontiera è stato considerato un rischio di sicurezza:

<http://www.schneier.com/blog/archives/2009/07/large_signs_a_s.html>

Una nuova, brillante truffa immobiliare:

<http://www.schneier.com/blog/archives/2009/07/new_real_estate.html>

Aggirare la crittografia di iPhone. Voglio più dettagli tecnici.

<<http://www.wired.com/gadgetlab/2009/07/iphone-encryption/>>

Eccellente scritto di Jonathan Zittrain sui rischi del cloud computing:

<<http://www.nytimes.com/2009/07/20/opinion/20zittrain.html>>

Il mio intervento sul cloud computing:

<http://www.schneier.com/blog/archives/2009/06/cloud_computing.html>

Altro allarmismo terroristico. Il titolo: "I terroristi potrebbero servirsi di Internet per sferrare un attacco nucleare: il resoconto". Sottotitolo: "Il rischio che il cyber-terrorismo aumenti al punto di diventare attacco nucleare cresce di giorno in giorno, secondo uno studio".

<<http://www.guardian.co.uk/technology/2009/jul/24/internet-cyber-attack-terrorists>>

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

Notare le espressioni evasive e ingannevoli nell'articolo. Lo studio "suggerisce che in presenza di condizioni favorevoli". Stiamo "lasciando aperta la possibilità". Il resoconto "delinea una serie di potenziali minacce e situazioni" in cui i criminali potrebbero "rendere più probabile un attacco nucleare". Santo cielo. Sono stufo di queste idiozie. Piantiamola di reagire in maniera eccessiva a rischi molto rari. Non lasciatevi terrorizzare.

<<http://www.schneier.com/essay-171.html>>

<<http://www.schneier.com/essay-124.html>>

Intervento interessante sulla sicurezza da parte di Eve Ensler sul sito TED. Non usa nessuno dei termini specifici, ma all'inizio riecheggia molto del pensiero attuale sulla psicologia evolutiva e la sua relazione con la sicurezza.

<http://www.ted.com/talks/eve_ensler_on_security.html>

In crittografia ci siamo serviti per molto tempo del termine 'snake oil' (lett. olio di serpente) in riferimento a sistemi crittografici con un buon battage pubblicitario ma che offrono ben poca sicurezza effettiva. È l'espressione che ho generalizzato in 'messinscena di sicurezza'. Beh, risulta che esiste davvero un venditore di olio di serpente.

<<http://blogs.reuters.com/oddly-enough/2009/07/24/we-found-him-he-really-exists/>>

oppure <<http://tinyurl.com/mo75tu>>

Una ricerca che dimostra quel che già sapevamo: troppi avvertimenti di sicurezza provocano compiacenza.

<<http://lorrie.cranor.org/pubs/sslwarnings.pdf>>

Il New York Times ha pubblicato un editoriale sulla regolamentazione delle centrali chimiche.

<<http://www.nytimes.com/2009/08/04/opinion/04tue2.html>>

Il problema è una classica esternalità di sicurezza, argomento che ho trattato nel 2007.

<<http://www.schneier.com/essay-194.html>>

Ottimo studio su sicurezza e usabilità: "When Security Gets in the Way" (Quando la sicurezza diventa un ostacolo).

<http://jnd.org/dn.mss/when_security_gets_in_the_way.html>

Una storia del 1934 sull'International Herald Tribune parla di come reagivamo all'imprevisto 75 anni fa:

<http://www.schneier.com/blog/archives/2009/08/how_we_reacted.html>

Una nuova falla di sicurezza aeroportuale: divertente.

<http://scienceblogs.com/gregladen/2009/07/overheard_at_airport.php>

Ecco una serie di consigli complicati su come proteggere le password che, scommetto, nessuno segue. Delle dieci regole elencate, non ne rispetto mai sette. E voi?

<<http://windowssecrets.com/2009/08/06/01-Gmail-flaw-shows-value-of-strong-passwords/>>

oppure <<http://tinyurl.com/px784h>>

I miei consigli su come scegliere password sicure.

<<http://www.wired.com/politics/security/commentary/securitymatters/2007/01/72458>>

oppure <<http://tinyurl.com/2beaq2>>

"An Ethical Code for Intelligence Officers" (Un codice etico per gli agenti dell'Intelligence).

<http://www.schneier.com/blog/archives/2009/08/an_ethical_code.html>

Un altro esempio di attacco man-in-the-middle:

<<http://www.schneier.com/blog/archives/2009/08/man-in-the-midd.html>>

"On Locational Privacy, and How to Avoid Losing it Forever" (Sulla locational privacy e come evitare di perderla per sempre).

<<http://www.eff.org/wp/locational-privacy>>

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

La sicurezza dei portatili alle frontiere

L'anno scorso ho parlato della propensione, in costante aumento, di alcuni governi fra cui Stati Uniti e Regno Unito, di controllare i contenuti dei computer portatili alle frontiere. Quel che sappiamo si basa ancora su aneddoti, dato che nessun paese ha chiarito le regolamentazioni che stabiliscono che cosa siano autorizzati a fare e a non fare gli agenti alle frontiere, né quali siano i diritti delle persone in questo frangente.

Aziende e privati hanno cercato di risolvere il problema in vari modi, dal non caricare dati sensibili sui portatili durante viaggi internazionali, al conservare le informazioni (criptate, ovviamente) su siti Web per poi scaricarle una volta giunti a destinazione. Soluzioni del genere non mi sono mai piaciute. Lavoro moltissimo in movimento, e ho sempre bisogno di portarmi appresso ogni genere di dati. Una gran quantità di dati, e scaricarla da un sito Web sicuro è un'operazione che necessita di molto tempo. E poi mi piace approfittare di lunghi voli internazionali per lavorare.

Esiste un'altra soluzione, che funziona con prodotti che criptano l'intero disco come PGP Disk (sono nel consiglio direttivo di PGP), TrueCrypt e BitLocker: criptare i dati verso una chiave che non conoscete.

Sembra folle, ma seguite il mio ragionamento. Attenzione: non provate a farlo se non avete dimestichezza con qualunque prodotto di crittografia state utilizzando. Il rischio è quello di ritrovarsi con un computer inservibile. Non prendetevela con me.

Passo 1: Prima di imbarcarvi sull'aereo, aggiungete un'altra chiave alla criptatura di tutto il disco (probabilmente si dovrà aggiungere un altro 'utente') e createla casuale. Con 'casuale' intendo proprio a casaccio: mettetevi a battere sui tasti per un po', come una scimmia che vuole scrivere Shakespeare. Non create una chiave facile da ricordare. Cercate di non memorizzarla affatto.

Tecnicamente questa chiave non cripta direttamente il disco rigido. Cripta invece la chiave utilizzata per criptare il disco rigido: ecco perché il software permette la multiutenza.

A questo punto abbiamo due utenti diversi con il nome di due chiavi distinte: quella che usate di solito, e una casuale appena inventata.

Passo 2: Inviatela la chiave casuale a qualcuno di cui vi fidate. Assicuratevi che il destinatario fidato sia in possesso della chiave, e assicuratevi che la chiave funzioni. Non potrete accedere al disco rigido senza di essa.

Passo 3: Distruggete, cancellate, disintegrate tutte le copie di quella nuova chiave casuale. Dimenticatela. Se è stata creata con un livello sufficiente di casualità e in maniera non facilmente memorizzabile, sarà affar semplice.

Passo 4: Imbarcatevi normalmente e utilizzate il vostro computer durante il volo.

Passo 5: Prima di atterrare, cancellate la chiave che usate di solito.

A questo punto non sarete in grado di avviare il computer. L'unica chiave rimasta è quella dimenticata al Passo 3. Non serve mentire all'agente di dogana, che spesso è già di per sé un reato; se non vi crede potete persino mostrargli una copia di questo articolo.

Passo 6: Quando avete passato la dogana, fatevi mandare la chiave dal vostro confidente, avviate il computer e riaggiungete la chiave che usate normalmente per accedere al disco rigido.

Ed è fatta.

Questo metodo non è certo una carta magica per passare facilmente un'ispezione doganale. Il vostro computer potrebbe essere sequestrato e potreste essere trascinati in tribunale e obbligati a rivelare chi è in possesso della chiave casuale.

Ma lo scopo di questo protocollo non è di prevenire una simile eventualità; è solo per evitare ogni possibile accesso al computer agli agenti doganali. Potreste essere trattenuti. Il vostro computer potrebbe essere confiscato (ciò vi costerà tutto il lavoro svolto durante il volo, ma onestamente a questo punto è l'ultimo dei problemi). Potreste essere respinti e rispediti a casa. Ma una volta a casa avrete accesso alla vostra amministrazione aziendale e ai vostri avvocati, nonché alla vostra prontezza di spirito e intelligenza dopo una buona notte di sonno e a tutti i diritti che normalmente avete nel paese in cui vi trovate.

Questa procedura non solo vi protegge da controlli senza mandato sui vostri dati alle frontiere, ma vi permette anche di negare a un agente di frontiera l'accesso ai dati senza dover mentire o fingere, che spesso è già questo un reato.

Ora il grosso interrogativo: a chi dovrete inviare la chiave casuale?

Certamente dev'essere qualcuno di cui vi fidate ma, ancor più importante, deve essere qualcuno con cui avete una relazione privilegiata. A seconda delle leggi del vostro paese, questi può essere il coniuge, un legale, un socio d'affari o il vostro parroco. In un'azienda di grandi dimensioni, il reparto IT potrebbe istituzionalizzare questa procedura, e l'help desk potrebbe tenere in custodia le chiavi.

Potreste anche inviare la chiave a voi stessi, ma fate attenzione. Se la spedite al vostro account webmail, allora direte una bugia all'ufficiale di dogana quando affermerete che non potete decrittare il disco rigido in alcun modo.

Potreste registrare la chiave in una chiavetta USB e inviarla alla vostra destinazione, ma è una soluzione passibile di errori e imprevisti. La chiavetta potrebbe non arrivare in tempo o non arrivare del tutto. Potreste inviarla due volte per posta aerea in due maniere diverse, e anche spedirla per fax... ma è tutto lavoro che preferisco non fare quando sono in viaggio.

Se vi interessa soltanto il viaggio di ritorno, potete impostarla prima di ritornare. O potete impostare un complesso sistema one-time pad, con elenchi identici di chiavi, uno con voi e l'altro a casa: distruggete ogni chiave sull'elenco che avete appresso ogni volta che la usate.

Ricordate che per fare in modo che questo funzioni dovrete installare e abilitare la crittografia dell'intero disco, utilizzando prodotti come PGP Disk, TrueCrypt o BitLocker.

Non credo arriveremo mai al punto in cui le informazioni sui nostri computer saranno completamente al sicuro alle frontiere internazionali. Anche se paesi come gli Stati Uniti e il Regno Unito chiarificheranno le loro regolamentazioni e istituiranno protezioni per la privacy, vi saranno sempre altri paesi che eserciteranno la propria autorità con maggior libertà. E a volte proteggere i nostri dati significa proteggerli da noi stessi.

Questo articolo è originariamente apparso su Wired.com.

<http://www.wired.com/politics/security/commentary/securitymatters/2009/07/securitymatters_0715>

oppure <<http://tinyurl.com/nw6bkd>>

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

Protocolli self-enforcing

Esistono svariati modi in cui due persone possono dividere un pezzo di torta a metà. Un modo è quello di trovare un'altra persona imparziale che lo faccia per loro. Questo metodo funziona, ma è necessaria appunto un'altra persona. Un altro sistema è che una delle due divida il pezzo di torta e che l'altra si lamenti (presso la polizia, un giudice, i genitori) se pensa che la divisione non sia giusta. Anche così funziona, ma richiede ancora una volta l'intervento di un terzo, almeno per risolvere eventuali dispute. Un terzo metodo è che una persona divida la torta e l'altra scelga la metà che vuole.

Quest'ultimo metodo, conosciuto dai bambini, dai fumatori di marijuana e da chiunque altro necessiti di dividere qualcosa velocemente e in modo equo, viene chiamato 'cut and choose' (letteralmente 'tagliare e scegliere'). La gente lo usa perché si tratta di un protocollo self-enforcing, ossia un protocollo ideato affinché nessuna delle due parti possa barare.

I protocolli self-enforcing sono utili perché non hanno bisogno di terze parti fidate. I sistemi moderni per il trasferimento di denaro (assegni, carte di credito, PayPal) richiedono intermediari fidati come banche e compagnie di carte di credito per facilitare il trasferimento. Anche i trasferimenti di contanti richiedono un governo fidato che emetta valuta, e si prendono una parte sotto forma di signoraggio. I moderni protocolli di contratto richiedono un sistema legale per risolvere le dispute. Prima che tali sistemi fossero istituiti e degni di fiducia, il commercio moderno non era possibile, e certi complessi contratti commerciali non sono ancora fattibili in aree prive di un sistema giudiziario equo. Il baratto è un protocollo self-enforcing: nessuno deve facilitare la transazione o risolvere dispute. Funziona e basta.

I protocolli self-enforcing sono più sicuri di altri perché i partecipanti non ottengono alcun vantaggio barando. Nei sistemi di voto attuali vi è parecchio potenziale per l'inganno, ma un'alzata di mani in una stanza, in cui ognuno presente nella stanza può verificare il conteggio, è self-enforcing. D'altro canto non esiste la segretezza del voto, i votanti che arrivano più tardi sono potenzialmente soggetti a coercizione, e non è un modello altrettanto efficace su vasta scala. Ma esistono protocolli di elezione matematici che possiedono proprietà self-enforcing, e alcuni crittografi ne hanno suggerito l'uso nelle elezioni.

Ecco un protocollo self-enforcing per stabilire la tassa di proprietà: il proprietario di una casa decide il valore della proprietà e calcola la tassa risultante, e il governo può accettare la tassa o acquistare la casa per quel prezzo. Suona poco realistico, ma il governo greco ha implementato esattamente questo sistema per tassare le antichità. Era il metodo più semplice per incentivare le persone a riportare accuratamente il valore dei pezzi antichi. E le cosiddette 'shotgun clause' nei contratti sono essenzialmente la stessa cosa.

L'IVA, cioè l'imposta sul valore aggiunto, è un'alternativa self-enforcing all'imposta sulle vendite. L'imposta sulle vendite viene raccolta sull'intero valore dell'oggetto alla vendita al dettaglio; sia il cliente che il negoziante vogliono ingannare il governo. Ma l'IVA viene raccolta a ogni passaggio dalla materia prima al cliente finale; è la differenza fra il prezzo dei materiali venduti e dei materiali acquistati. I compratori vogliono ricevere ufficiali con un prezzo d'acquisto il più alto possibile, così che ogni compratore lungo la catena assicura l'onestà del venditore. Certo, vi è sempre un incentivo all'inganno nella vendita finale al cliente, ma la quantità di imposte raccolte a quel punto è molto più bassa.

Naturalmente i protocolli self-enforcing non sono perfetti. Per esempio, qualcuno in un 'cut and choose' può dare un pugno all'altra persona e scappare con tutta la torta. Ma qui l'obiettivo non è la perfezione; lo scopo è ridurre l'inganno eliminando possibili metodi di inganno. I protocolli self-enforcing migliorano la sicurezza non attraverso l'implementazione di contromisure atte a prevenire inganni e raggiri, ma facendo leva su incentivi economici che invitino entrambe le parti a non barare.

Un ultimo esempio di protocollo self-enforcing. Immaginate una nave pirata che si imbatte in una tempesta. I pirati sono tutti preoccupati per il loro oro, perciò ognuno di essi mette la borsa con il suo oro nella cassaforte comune. Durante la tempesta la cassaforte si rompe, si apre e l'oro di tutti si mescola e finisce sul pavimento. Come fanno i pirati a stabilire chi possiede cosa? Ognuno di essi annuncia al gruppo la quantità d'oro che possedeva. Se il totale dell'oro dichiarato equivale all'oro presente nella pila, viene diviso secondo le quantità annunciate da ogni pirata. Se le quantità differiscono, il capitano si tiene tutto l'oro. Vi sono molti modi in cui questo sistema può fallire: il capitano e un pirata possono mettersi d'accordo per far sballare il totale, per esempio. Ma è comunque un sistema self-enforcing atto a scongiurare eventuali false dichiarazioni dei singoli pirati.

Questo articolo è originariamente apparso su ThreatPost.
<<http://threatpost.com/blogs/value-self-enforcing-protocols>>

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

Le news su Schneier

Interverrò al meeting OWASP a Minneapolis il 24 agosto:
<http://www.owasp.org/index.php/Minneapolis_St_Paul>

Qui potete trovare la registrazione audio del mio intervento alla Black Hat Conference:
<<http://www.blackhat.com/html/bh-usa-09/bh-usa-09-archives.html#Schneier>>
oppure <<http://tinyurl.com/mvewwx>>

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

Un altro nuovo attacco contro AES

È stato da poco annunciato un nuovo attacco davvero impressionante contro AES.

Negli ultimi due mesi sono apparsi due nuovi studi crittanalitici su AES. Gli attacchi presentati negli studi non sono fattibili: sono troppo complessi, sono attacchi related-key e sono contro versioni di AES a chiave più estesa e non contro la versione a 128 bit utilizzata dalla maggior parte delle implementazioni; ma si tratta comunque di lavori impressionanti.

Questo nuovo attacco, studiato da Alex Biryukov, Orr Dunkelman, Nathan Keller, Dmitry Khovratovich e Adi Shamir, è assai più devastante. È un attacco assolutamente pratico contro AES-256 a dieci round:

“Abstract. AES è il block cipher meglio conosciuto e più diffuso. Le sue tre versioni (AES-128, AES-192 e AES-256) differiscono nella lunghezza delle loro chiavi (128 bit, 192 bit e 256 bit) e nel numero di round (rispettivamente 10, 12 e 14). Nel caso di AES-128 non esiste un attacco più veloce della complessità 2^{128} della ricerca esaustiva. Tuttavia, è stato recentemente dimostrato che AES-192 e AES-256 possono essere compromessi da attacchi che richiedono un tempo di 2^{176} e 2^{119} rispettivamente. Malgrado queste complessità siano molto più veloci della ricerca esaustiva, sono anche completamente impraticabili e non sembrano rappresentare alcuna reale minaccia alla sicurezza di sistemi basati su AES.

“In questo studio descriviamo svariati attacchi che possono compromettere con complessità pratica quelle varianti di AES-256 il cui numero di round è paragonabile a quello di AES-128. Uno dei nostri attacchi si serve soltanto di due related key e di un tempo di 2^{39} per recuperare la chiave a 256 bit completa di una versione a 9 round di AES-256 (il miglior attacco precedente ai danni di questa variante richiedeva 4 related key e un tempo di 2^{120}). Un altro attacco può compromettere una versione a 10 round di AES-256 in un tempo di 2^{45} , ma sfrutta un tipo più forte di attacco related subkey (il miglior attacco precedente ai danni di questa variante richiedeva 64 related key e un tempo di 2^{172})”.

Gli autori descrivono inoltre un attacco contro AES-256 a 11 round che richiede un tempo di 2^{70} : quasi pratico.

Questi nuovi risultati migliorano nettamente quanto ottenuto dagli studi di Biryukov, Khovratovich e Nikolic menzionati in precedenza, e sono un deciso passo avanti anche rispetto a uno studio che ho elaborato insieme ad altri sei autori nel 2000, in cui descriviamo un attacco related key contro AES-256 a 9 round (allora chiamato Rijndael) in 2^{224} . (Questo ancora una volta dimostra il vecchio adagio del crittografo: gli attacchi migliorano in continuazione, non peggiorano mai).

Da qualsiasi punto di vista, questo è un risultato di enorme importanza.

Vi sono tre motivi per non lasciarsi prendere dal panico:

* L'attacco sfrutta il fatto che la programmazione delle chiavi per la versione a 256 bit è piuttosto scadente (un dettaglio che avevamo fatto notare nel nostro studio del 2000) ma non si estende ad AES con chiave a 128 bit.

* Si tratta di un attacco related key, che richiede che il crittanalista abbia accesso a testi in chiaro criptati con una serie di chiavi fra loro relazionate in maniera specifica.

* L'attacco compromette solo 11 round di AES-256. La versione completa di AES-256 ha 14 round.

Non è molto confortante, sono d'accordo, ma è quanto abbiamo.

La crittografia è tutta una questione di margini di sicurezza. Se è possibile compromettere n round di un cipher, lo si progetta con 2n o 3n round. Quel che stiamo osservando ora è che il margine di sicurezza di AES è molto minore di quanto si credeva in precedenza. E se da un lato non c'è motivo di scartare AES a favore di un altro algoritmo, il NST dovrebbe aumentare il numero di round di tutte e tre le varianti AES. A questo punto suggerisco AES-128 a 16 round, AES-192 a 20 round e AES-256 a 28 round. O magari anche di più, per evitare di revisionare lo standard in continuazione.

E per quanto riguarda nuove applicazioni, suggerisco di non usare AES-256. Per il prossimo futuro AES-128 offre un margine di sicurezza più che sufficiente. Ma se si sta già utilizzando AES-256 non c'è ragione di cambiare.

Lo studio:

<<http://eprint.iacr.org/2009/374>>

Precedenti studi di crittanalisi AES:

<<http://eprint.iacr.org/2009/241>>

<<http://eprint.iacr.org/2009/317>>

AES:

<<http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>>

<http://www.schneier.com/blog/archives/2009/07/new_attack_on_a.html>

<<http://www.schneier.com/paper-rijndael.pdf>>

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

Lo scassinamento delle serrature e Internet

Le serrature fisiche non sono molto efficaci. Servono a proteggerci dagli onesti, ma qualsiasi scassinatore che si definisca tale può forzare una comune serratura molto velocemente.

Una volta la maggior parte delle persone non lo sapeva. Certo, tutti vedevamo film e telefilm dove criminali e investigatori privati scassinavano serrature e lucchetti con una facilità incredibile e pensavamo fosse realistico, ma in un certo senso ci faceva piacere pensare che le nostre serrature potessero proteggerci dagli intrusi.

Internet ha cambiato tutto questo.

Prima è apparsa la MIT Guide to Lockpicking (Guida allo scassinamento delle serrature) scritta dal defunto Bob ('Ted the Tool') Baldwin. Poi è stato pubblicato lo studio del 2003 di Matt Blaze su come compromettere sistemi a chiave universale. In seguito la Rete fu invasa da una serie di informazioni sullo scassinamento di serrature: come aprire il lucchetto di una bicicletta con una penna Bic, il key bumping, e molto altro.

Molte di queste tecniche erano già note sia nella comunità criminale che in quella dei fabbri. I fabbri hanno tentato di sopprimere queste informazioni, credendo che la loro segretezza corporativa era migliore dell'apertura e della divulgazione. Ma hanno perso: non vi sono mai state in circolazione così tante informazioni sullo scassinamento di serrature e casseforti accessibili al pubblico come adesso.

Le aziende costruttrici di serrature hanno risposto con serrature più complicate e con campagne di disinformazione altrettanto complicate.

Pare che esista un limite alla sicurezza di una serratura interamente meccanica, e un limite per quanto riguarda le dimensioni e la praticità di una chiave perché venga accettata dal pubblico. Di conseguenza è aumentato l'interesse verso altre tecnologie di costruzione delle serrature.

In qualità di tecnologo della sicurezza, mi preoccupa il fatto che se non comprendiamo appieno queste nuove tecnologie e le nuove tipologie di vulnerabilità che portano con sé, potremmo abbandonare una tecnologia mediocre in cambio di una ancora peggiore. Le serrature elettroniche sono vulnerabili agli attacchi, spesso in modalità nuove e sorprendenti.

Cominciamo dai tastierini numerici, sempre più comuni sulle porte di casa. Il loro vantaggio è che non è necessario portarsi appresso una chiave, ma il problema è che non si può prestare la chiave di casa a qualcuno per un giorno e poi riprenderla il giorno dopo. Pertanto la sicurezza degrada col tempo: più viene utilizzato il tastierino, più persone sanno come entrare. Tastierini elettronici più complessi sono dotati di una serie di opzioni per evitare questo inconveniente, ma i tastierini elettronici funzionano solo quando c'è corrente, e quelli alimentati da batterie hanno anch'essi i loro punti deboli. Inoltre, troppe persone non si prendono la briga di modificare il codice di accesso predefinito.

I tastierini presentano anche altre falle di sicurezza. Noto con frequenza tastierini in cui quattro dei dieci pulsanti sono più consumati degli altri sei. Consumati dall'uso, ovviamente, e invece di 10.000 combinazioni possibili, ora devo provarne soltanto 24.

I lettori di impronte digitali rappresentano una tecnologia alternativa, ma anche in questo caso vi è tutta una serie di problemi di sicurezza noti. E presentano anche inconvenienti operativi: sono difficili da utilizzarsi al freddo o quando si hanno le mani sudate; e lasciare una chiave al vicino di casa per far entrare l'idraulico comincia ad apparire una storia di spionaggio.

Alcune aziende si spingono ancora più in là. Qualche mese fa, Schlage ha introdotto una serie di serrature che possono venire aperte da una chiave, da un codice a quattro cifre, o anche da Internet. Proprio così, la serratura è online. Si possono inviare messaggi SMS alla serratura o comunicare con essa attraverso un sito Web, e la serratura può inviarvi messaggi quando qualcuno la apre o se qualcuno tenta invano di aprirla.

Sembra una bella idea, ma mettere una serratura su Internet causa tutta una nuova serie di problemi, nessuno dei quali possiamo capire interamente. Ancora peggio: la sicurezza è forte quanto l'anello più debole. Il sistema di Schlage combina la 'scassinabilità' intrinseca di una serratura fisica, le nuove vulnerabilità dei tastierini

elettronici, e il rischio di hacking online. Per la maggior parte delle applicazioni, è un rischio semplicemente troppo grande.

Questo articolo è originariamente apparso su DarkReading.com.
<<http://www.darkreading.com/blog/archives/2009/08/locks.html>>

Una copia di questo articolo, con i rimandi integrati nel testo, è disponibile sul mio blog:
<http://www.schneier.com/blog/archives/2009/08/lockpicking_and.html>

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

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 SpA

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

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

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

Per informazioni <crypto-gram@communicationvalley.it>

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

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

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

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

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

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

Copyright (c) 2009 - Bruce Schneier.