

CRYPTO-GRAM  
15 luglio 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 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:

- Immaginare le minacce
- La sicurezza, le dimensioni di un gruppo, e il cervello umano
- Gli attacchi cibernetici della Corea del Nord
- Perché le persone non comprendono i rischi
- Frode su eBay
- News
- Autenticare i documenti cartacei
- I pro e i contro del mascheramento della password
- I "costi occulti" della privacy
- Sistemare la sicurezza aeroportuale
- Le news su Schneier
- Una svolta nell'ambito della crittografia omomorfica
- Nuovo attacco contro AES
- MD6 ritirato dal concorso SHA-3
- Risultati crittanalitici ancora migliori contro SHA-1
- Commenti dei lettori

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

Immaginare le minacce

Un paio di anni fa, il Dipartimento per la Sicurezza Nazionale invitò un gruppo di scrittori di fantascienza per una giornata, e diede loro il compito di pensare a dei modi con i quali i terroristi avrebbero potuto attaccare l'America. Se la nostra incapacità nel prevenire l'11 settembre ha segnato una grave mancanza di immaginazione, come alcuni affermarono all'epoca, allora chi meglio degli scrittori di fantascienza avrebbe potuto instillare un po' d'immaginazione in ambito antiterroristico?

A quel tempo considerai tale esercizio di poco conto e lo definii 'imbarazzante'. Non ho mai creduto che l'11 settembre sia accaduto per mancanza di immaginazione. Ritenni, e ritengo tuttora, che l'11 settembre sia stato soprattutto il punto di convergenza di tre cose: il doppio fallimento del coordinamento centralizzato e del controllo locale all'interno dell'FBI, e alcuni colpi di fortuna degli aggressori. Più immaginazione porta a un maggior numero di minacce da trama cinematografica -- il che a sua volta va ad aumentare la paura generale e porta a sopravvalutare i rischi. E non aiuta affatto a mantenerci al sicuro.

Recentemente ho letto uno studio di Magne Jørgensen che offre alcuni spunti sul perché questo accada. Intitolato "More Risk Analysis Can Lead to Increased Over-Optimism and Over-Confidence" (Un'analisi dei rischi sempre più approfondita può portare a un eccessivo ottimismo e a un'eccessiva fiducia in se stessi), questo studio non parla affatto di terrorismo. Si occupa invece dei progetti software.

La maggior parte dei progetti di sviluppo software sono eccessivamente ottimistici, e moltissimi progettisti hanno troppa fiducia nei loro piani eccessivamente ottimistici. Jørgensen ha studiato come questo sia influenzato dall'analisi dei rischi. Ha condotto quattro esperimenti distinti su ingegneri software e (anche se vi sono molti avvertimenti nello studio, ed è necessario effettuare ulteriori ricerche) ha concluso che eseguire un'eccessiva analisi dei rischi può portare gli ingegneri a essere troppo ottimisti invece che più realisti.

Tutte le spiegazioni potenziali provengono dall'economia comportamentale: bias cognitivi che influenzano il nostro modo di pensare e di prendere decisioni. (Ho scritto in merito ad alcuni di questi bias e di come condizionano le decisioni di sicurezza, e vi è anche un libro eccellente sull'argomento).

In primo luogo esiste un bias di controllo. Tendiamo a sottovalutare i rischi in situazioni in cui abbiamo il controllo, e a sopravvalutare i rischi in situazioni in cui non abbiamo il controllo. Un esempio tipico: guidare l'automobile e viaggiare in aereo. Tale bias si fortifica con la familiarità, il coinvolgimento e il desiderio di sperimentare il controllo, tutti elementi che si intensificano con l'intensificarsi dell'analisi dei rischi. Pertanto, più analisi dei rischi porta a un maggiore bias di controllo, che a sua volta porta a una maggiore sottovalutazione dei rischi.

La seconda spiegazione è l'euristica della disponibilità. In sostanza, giudichiamo l'importanza o la probabilità di qualcosa che accade dalla facilità con cui riusciamo a pensare a esempi di quel qualcosa. Per cui tendiamo a sopravvalutare la probabilità di un rischio raro presentato nel titolo di una notizia, perché è molto facile da immaginare. Analogamente, sottovalutiamo la probabilità di eventi che non vengono riportati dalle news.

Un corollario di questo fenomeno: quando ci viene chiesto di pensare a una serie di cose, sopravvalutiamo la probabilità dell'ultima cosa pensata perché la si ricorda più facilmente.

Secondo il ragionamento di Jørgensen, si tende a effettuare l'analisi dei rischi software pensando prima ai rischi gravi, e poi a quelli più gestibili. Pertanto, maggiore è l'analisi dei rischi, meno grave sarà l'ultimo rischio immaginato, e dunque maggiore sarà la sottovalutazione del rischio totale.

La terza spiegazione è simile: la cosiddetta 'regola del picco e della fine' (peak end rule). Quando si ripensa a una esperienza completa, in genere si tende a dare troppo peso all'ultima parte dell'esperienza. In un esperimento i soggetti dovevano tenere le mani sotto l'acqua fredda per un minuto. Poi dovevano tenere ancora le mani sotto l'acqua fredda per un minuto e successivamente tenere le mani sotto l'acqua per altri 30 secondi mentre la temperatura veniva gradualmente innalzata. Quando è stato chiesto ai soggetti di ricordare l'esperienza, la maggioranza ha preferito la seconda opzione rispetto alla prima, anche se la seconda opzione presentava un maggior disagio globale. (Un attrezzo medico invasivo è stato riprogettato in maniera analoga, provocando un periodo di disagio più lungo, eccetto gli ultimi secondi in cui l'esperienza si faceva un po' più gradevole. Ai soggetti è piaciuto molto di più). Questo, come la seconda spiegazione vista prima, significa che il rischio immaginato meno grave che appare cronologicamente per ultimo riceve più considerazione di quanta meriterebbe.

Tutto davvero affascinante. Ma i bias producono l'effetto opposto quando si tratta di minacce da trama cinematografica. Più si pensa a possibilità terroristiche inverosimili, più diventano assurde e spaventose, e si pensa di avere sempre minor controllo su di esse. Questo induce a sopravvalutare i rischi.

Si pensi a tutto questo nel contesto del terrorismo. Se vi si chiede di pensare a delle minacce, immaginerete innanzi tutto le più gravi. Se siete spinti a trovarne altre, se assumete degli scrittori di fantascienza per inventarle, vi troverete presto nella sfera delle minacce da trama cinematografica a bassa probabilità. Ma dato che sono cronologicamente le ultime a venir pensate, sono più facilmente richiamabili. (E sono anche le più vivide -- chi scrive di fantascienza fa un ottimo lavoro in tal senso -- altro fattore che ci porta a sopravvalutarne la probabilità). Sono inoltre minacce che ci fanno credere di aver meno controllo della situazione di quanto crediamo. Passare troppo tempo a immaginare scenari disastrosi porta a sopravvalutare i rischi di un disastro.

Sono certo vi sia anche in atto un ancoraggio psicologico. Si tratta di un altro bias cognitivo, in cui le stime numeriche vengono influenzate dalle cifre alle quali si è pensato più recentemente, anche casuali. Soggetti a cui viene dato un elenco di tre rischi penseranno che il numero totale di rischi è minore rispetto ai soggetti a cui viene dato un elenco di dodici rischi. Quindi se il gruppo di scrittori di fantascienza riesce a elaborare 137 rischi, la gente sarà portata a pensare che il numero di rischi è maggiore di quel che normalmente penserebbe -- anche se la cifra 137 viene riconosciuta come assurda.

Jørgensen non ritiene che l'analisi dei rischi sia inutile nei progetti software, come io non trovo inutile fare un brainstorming su possibili scenari in ambito antiterroristico. Entrambi i sistemi possono portare a nuovi spunti e a nuove scoperte e, di conseguenza, a una analisi più intelligente sia dei rischi specifici che di quelli più generali. Ma affidarsi troppo a questi procedimenti può risultare nocivo.

Il mese scorso, alla 2009 Homeland Security Science & Technology Stakeholders Conference che si è tenuta a Washington D.C., gli scrittori di fantascienza hanno aiutato i partecipanti a pensare diversamente alla sicurezza. Questo mi sembra un utilizzo migliore del loro talento che non immaginare alcuni fra i trilioni di sistemi con cui i terroristi possono attaccare l'America.

Rimandi:

<[http://www.wired.com/dangerroom/2007/05/homeland\\_security/](http://www.wired.com/dangerroom/2007/05/homeland_security/)>  
<[http://www.usatoday.com/tech/science/2007-05-29-deviant-thinkers-security\\_N.htm?csp=34](http://www.usatoday.com/tech/science/2007-05-29-deviant-thinkers-security_N.htm?csp=34)>  
<[http://www.theregister.co.uk/2007/05/31/sci\\_fi\\_consultants\\_at\\_the\\_dhs/](http://www.theregister.co.uk/2007/05/31/sci_fi_consultants_at_the_dhs/)>  
<<http://www.schneier.com/essay-087.html>>  
<<http://simula.no/research/engineering/publications/Simula.SE.621>>  
<<http://www.schneier.com/essay-155.html>>  
<[http://www.schneier.com/blog/archives/2009/04/book\\_review\\_the.html](http://www.schneier.com/blog/archives/2009/04/book_review_the.html)>  
<[http://www.schneier.com/blog/archives/2007/05/rare\\_risk\\_and\\_o\\_1.html](http://www.schneier.com/blog/archives/2007/05/rare_risk_and_o_1.html)>  
<<http://www.google.com/search?q=movie+plot+threats+site:schneier.com>>  
<<http://www.washingtonpost.com/wp-dyn/content/article/2009/05/21/AR2009052104379.html>>  
<[http://www.wired.com/politics/security/commentary/securitymatters/2009/06/securitymatters\\_0619](http://www.wired.com/politics/security/commentary/securitymatters/2009/06/securitymatters_0619)>

Questo articolo è originariamente apparso su Wired.com:

<[http://www.wired.com/politics/security/commentary/securitymatters/2009/06/securitymatters\\_0619](http://www.wired.com/politics/security/commentary/securitymatters/2009/06/securitymatters_0619)>  
oppure <<http://tinyurl.com/nm6tj7>>

Una copia di questo articolo, con i rimandi integrati nel testo, è disponibile sul mio blog:  
<[http://www.schneier.com/blog/archives/2009/06/imagining\\_threa.html](http://www.schneier.com/blog/archives/2009/06/imagining_threa.html)>

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

La sicurezza, le dimensioni di un gruppo, e il cervello umano

Se le dimensioni della vostra azienda superano le 150 persone, è arrivato il momento di utilizzare dei badge identificativi. Questo non perché gruppi più estesi siano in qualche modo meno sicuri, ma perché pare che 150 sia il limite cognitivo al numero di persone con cui una mente umana può mantenere una relazione sociale coerente.

Il primatologo Robin Dunbar ha derivato questo numero confrontando il volume del neocortex (la parte 'pensante' del cervello di un mammifero) con le dimensioni dei gruppi sociali dei primati. Analizzando i dati di 38 classi di primati e facendo una proiezione considerando le dimensioni del neocortex umano, ne ha dedotto una 'dimensione media di gruppo' di circa 150 individui.

Tale numero compare con regolarità nella società umana: è la dimensione stimata di un villaggio agricolo del Neolitico, la dimensione in cui si suddividono gli insediamenti degli Ittiti, e l'unità di base negli eserciti professionisti dall'epoca romana ai giorni nostri. Gruppi più estesi non sono ugualmente stabili poiché i loro membri non si conoscono

abbastanza bene. Invece di pensare ai membri come a persone, li si considera gruppi di persone. Perché tali gruppi funzionino bene, è necessaria una struttura imposta dall'esterno, come appunto l'utilizzo di badge identificativi.

Ovviamente i badge non sono l'unico sistema per determinare uno status di appartenenza/non appartenenza a un gruppo. Altri indicatori possono essere distintivi, uniformi, e strette di mano segrete. Hanno diverse proprietà di sicurezza, e alcuni hanno più senso di altri a livelli diversi di tecnologia, ma una volta che un gruppo raggiunge le 150 persone si deve fare qualcosa.

Più in generale, esistono svariati livelli di dimensioni naturali di gruppi umani, che aumentano con un coefficiente di tre, all'incirca: 5, 15, 50, 150, 500 e 1500; anche se in realtà i numeri non sono così precisi, e quei gruppi meno incentrati sulla sopravvivenza tendono a essere più ristretti. I livelli si riferiscono sia all'intensità e all'intimità dei rapporti, che alla frequenza di contatto.

Il gruppo più piccolo, da tre a cinque, è una 'cricca': il numero di persone a cui chiedere aiuto nei momenti di grave difficoltà emotiva. Il gruppo da dodici a venti unità è il "gruppo di affinità": persone con le quali abbiamo legami speciali. Dopo di che abbiamo il gruppo da 30 a 50, la dimensione tipica degli accampamenti notturni di cacciatori e raccoglitori, generalmente estratti dallo stesso gruppo di 150 persone. A prescindere dalla grandezza dell'azienda per cui lavoriamo, vi sono soltanto 150 persone all'incirca che consideriamo 'colleghi'. (Nelle piccole imprese, Alice e Bob gestiscono la contabilità. In compagnie più grandi troviamo il reparto contabilità, all'interno del quale magari conosciamo qualcuno di persona). Il gruppo di 500 persone è la 'megabanda' e il gruppo da 1.500 è la 'tribù'. Millecinquecento è approssimativamente il numero di volti che possiamo riconoscere, e la dimensione tipica di una società di cacciatori e raccoglitori.

Questi numeri si riflettono nell'organizzazione militare attraverso la storia: squadre di 10-15 unità organizzate in plotoni di tre o quattro squadre, organizzati in compagnie di tre o quattro plotoni, organizzate in battaglioni di tre o quattro compagnie, organizzati in reggimenti di tre o quattro battaglioni, organizzati in divisioni di due o tre reggimenti, organizzate in corpi di due o tre divisioni.

La coesione può diventare un problema serio quando le organizzazioni raggiungono e superano i 150 individui. Superato il limite di 150, i gruppi presentano una maggiore infrastruttura imposta dall'esterno, e sistemi di sicurezza maggiormente formalizzati. In gruppi ristretti, la sicurezza è pressoché interamente ad hoc. Compagnie formate da meno di 150 persone non si preoccupano di usare badge identificativi; aziende con più di 500 persone assumono una guardia che siede all'ingresso e controlla i badge. I militari hanno secoli di esperienza alle spalle, e in circostanze piuttosto dure, ma anche in questo contesto il vero impegno e la formazione di legami stretti avvengono invariabilmente al livello della compagnia. Al di sopra di esso è necessario imporre ranghi basandosi sulla disciplina.

Tutto il confronto fra dimensioni e cervello umano potrebbe essere una sciocchezza, e molti psicologi evolutivisti sono in disaccordo. Ma di certo i sistemi di sicurezza sono più formalizzati quando i gruppi aumentano di numero e i membri si conoscono sempre meno. Quando vengono stabiliti sistemi più formali di risoluzione delle dispute: gli anziani del villaggio, i magistrati, i giudici? Qual è il limite raggiunto il quale sistemi formali di autenticazione diventano obbligatori? Le piccole aziende possono andare

avanti senza moduli interni, senza memo e altre procedure necessarie alle grandi imprese; a che punto cambiano le cose? Come viene formalizzato il sistema punitivo all'aumentare della dimensione del gruppo? E come tutti questi elementi condizionano la coesione del gruppo? Le persone si comportano in maniera differente su siti di social networking come Facebook quando la loro lista di 'amici' si espande e diviene meno intima. Commercianti locali a volte permettono ai clienti abituali di 'mettere in conto' e di non pagare immediatamente. Io presto libri ai miei amici con molta meno formalità di una biblioteca pubblica. Che altri esempi avete notato?

Una versione rivista di questo articolo, senza link, è apparsa nel numero di Luglio/Agosto 2009 di IEEE Security & Privacy.

Rimandi:

<[http://www.cracked.com/article\\_14990\\_what-monkeysphere.html](http://www.cracked.com/article_14990_what-monkeysphere.html)>

<<http://arxiv.org/abs/cond-mat/0403299>>

<[http://www.army.mil/usapa/epubs/pdf/p10\\_1.pdf](http://www.army.mil/usapa/epubs/pdf/p10_1.pdf)>

<[http://online.wsj.com/article/SB119518271549595364.html?mod=googlenews\\_wsj](http://online.wsj.com/article/SB119518271549595364.html?mod=googlenews_wsj)>

Una copia di questo articolo, con i rimandi integrati nel testo, è disponibile sul mio blog: <[http://www.schneier.com/blog/archives/2009/07/security\\_group.html](http://www.schneier.com/blog/archives/2009/07/security_group.html)>

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

### Gli attacchi cibernetici della Corea del Nord

A sentire i media, gli Stati Uniti hanno subito un grave attacco cibernetico la scorsa settimana. Le storie erano dovunque. Il Wall Street Journal titolava "Un cyber-blitz colpisce gli USA: la Corea". La colpa è stata data alla Corea del Nord.

Dove eravate quando la Corea del Nord attaccò l'America? Avete sentito la furia delle truppe nordcoreane? Temevate per il destino del vostro paese? O la vostra determinazione si è rafforzata ancor di più, sapendo che avremmo difeso la nostra patria, con coraggio e valore?

Secondo me neanche ve ne siete accorti, e (a meno di non leggere un giornale o un sito Web di news) non avevate la più vaga idea che stesse accadendo qualcosa. Certo, qualche sito Web governativo è stato messo fuori servizio, ma non è un'eventualità preoccupante, né infrequente. Altri siti Web del governo sono stati attaccati ma si sono difesi, come del resto accade spesso. Se questo è come dovrebbe essere un attacco cibernetico internazionale, non sembra valga la pena di preoccuparsi tanto.

Attacchi cibernetici spinti da motivazioni politiche non sono affatto una novità. Abbiamo visto il Regno Unito contro l'Irlanda, Israele contro gli stati arabi, La Russia contro diverse ex-repubbliche sovietiche, l'India contro il Pakistan (specie dopo i test nucleari del 1998), la Cina contro gli Stati Uniti (specie nel 2001, quando un aereo spia statunitense entrò in collisione con un caccia cinese). E così via.

Un attacco cibernetico notevole è avvenuto nel 2007, quando il governo estone venne attaccato nel cyberspazio a seguito di un incidente diplomatico con la Russia sul trasferimento di un monumento sovietico della Seconda Guerra Mondiale. Le reti di

molte organizzazioni estoni, fra cui il parlamento estone, banche, ministeri, giornali ed enti televisivi sono state attaccate e in molti casi messe fuori uso. L'Estonia ha immediatamente accusato la Russia, e la Russia ha immediatamente negato qualsiasi coinvolgimento.

Di questo caso si è parlato in termini sensazionalistici come della prima guerra cibernetica, ma a distanza di due anni non sono ancora emerse prove che il governo russo sia responsabile. Malgrado gli hacker russi siano stati innegabilmente fra i maggiori istigatori dell'attacco, gli unici individui che sono stati identificati con certezza sono dei giovani di origine russa residenti in Estonia, irritati per l'incidente del monumento storico.

Andando più a fondo in questi incidenti internazionali si scopre che in sostanza si tratta di ragazzini che giocano alla politica. Mercoledì scorso, il servizio di intelligence nazionale della Corea del Sud ha ammesso di non sapere affatto che la Corea del Nord era responsabile degli attacchi: "La Corea del Nord o simpatizzanti nordcoreani al Sud", sono state le sue parole. Ancora una volta, si tratterà di ragazzini che giocano alla politica.

Con questo non intendo dire che gli attacchi cibernetici effettuati dai governi non siano un problema, o che la guerra cibernetica sia un fenomeno da ignorare. I costanti attacchi a opera di cittadini cinesi contro le reti statunitensi non saranno sponsorizzati dal governo, ma è piuttosto evidente che vengano tacitamente approvati. I criminali, dagli hacker solitari ai gruppi organizzati, attaccano reti in continuazione. E la guerra si estende a ogni possibile contesto: terra, mare, aria, spazio e ora al cyberspazio. Ma il terrorismo cibernetico non è altro che un'invenzione dei media con lo scopo di spaventare la gente. E per esservi una guerra cibernetica, deve esservi prima una guerra vera e propria.

Israele sta al momento considerando di attaccare l'Iran nel cyberspazio, per esempio. Se ci prova, scoprirà che attaccare le reti di computer è un disturbo per le installazioni nucleari che sta prendendo di mira, ma è ben lungi dall'essere un danno equivalente al bombardarle.

In maggio, il presidente Obama ha tenuto un discorso molto importante sulla sicurezza cibernetica. Ha ragione quando dice che la sicurezza cibernetica è un problema di sicurezza nazionale, e che il governo deve fare di più per prevenire attacchi cibernetici, ma non ha potuto trattenersi dall'alimentare la minaccia con storie di terrore: "In uno degli incidenti cibernetici più gravi mai visti contro i nostri network militari, molte migliaia di computer sono stati infettati lo scorso anno da software malevolo -- il malware", ha affermato. Però non ha detto che tali infezioni sono state dovute al fatto che l'Air Force non si è presa la briga di tenere aggiornate le patch.

Questo è il volto della guerra cibernetica: attacchi facilmente prevenibili che, anche quando hanno successo, vengono notati da poche persone. Anche l'attuale incidente pare che sia in realtà un worm di cinque anni fa malamente modificato; nessuna rete moderna dovrebbe essere ancora vulnerabile a malware come questo.

Proteggere le nostre reti non richiede una qualche avanzata e segreta tecnologia in stile NSA. Bastano quei noiosi compiti di amministrazione della sicurezza di rete che sappiamo già come effettuare: mantenere le patch aggiornate, installare un buon software anti-malware, configurare correttamente i firewall e i sistemi antintrusione,

monitorare le reti. E mentre alcune reti governative e aziendali fanno un ottimo lavoro in questo senso, altre continuano a commettere errori.

Basta con i sensazionalismi e gli strepiti. La notizia vera non sono gli attacchi, ma che alcune reti avevano implementata una sicurezza sufficientemente mediocre da essere vulnerabili a tali attacchi.

Rimandi:

<<http://www.google.com/hostednews/ap/article/ALeqM5iaaWwzg--SOmIz9Qjdju4UYFB5GgD99ABC700>>

<<http://www.google.com/hostednews/afp/article/ALeqM5hM1x-CC9vCIHGSq6RSvkKHZaZ5sg>>

<<http://online.wsj.com/article/SB124701806176209691.html>>

<<http://government.zdnet.com/?p=5093>>

<[http://news.yahoo.com/s/ap/20090708/ap\\_on\\_re\\_as/as\\_skorea\\_cyber\\_attack](http://news.yahoo.com/s/ap/20090708/ap_on_re_as/as_skorea_cyber_attack)>

<<http://www.reuters.com/article/idUSTRE5663EC20090707>>

<[http://www.businessweek.com/the\\_thread/techbeat/archives/2009/07/why\\_is\\_the\\_g ove.html](http://www.businessweek.com/the_thread/techbeat/archives/2009/07/why_is_the_g ove.html)>

<<http://www.wired.com/threatlevel/2009/07/show-of-force/>>

<[http://www.businessweek.com/the\\_thread/techbeat/archives/2009/07/why\\_is\\_the\\_g ove.html](http://www.businessweek.com/the_thread/techbeat/archives/2009/07/why_is_the_g ove.html)>

Questo articolo è apparso originariamente sul sito Web della Minnesota Public Radio.

<<http://minnesota.publicradio.org/display/web/2009/07/10/schneier/>>

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

<[http://www.schneier.com/blog/archives/2009/07/north\\_korean\\_cy.html](http://www.schneier.com/blog/archives/2009/07/north_korean_cy.html)>

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

Perché le persone non comprendono i rischi

Il Minneapolis Star Tribune della scorsa settimana aveva questo titolone in prima pagina: "Il co-sleeping uccide circa 20 neonati ogni anno" ('co-sleeping' è l'abitudine di dormire con i propri figli nello stesso letto). L'unico problema è che non è stata fornita nessuna informazione aggiuntiva che potesse aiutare a comprendere la statistica.

Quanti neonati non muoiono ogni anno? Quanti neonati che dormono in letti separati muoiono ogni anno? Il tasso di morte dei bambini che dormono insieme ai genitori è maggiore o minore rispetto a quello dei bambini che dormono separatamente? Senza queste informazioni è impossibile sapere se questo dato statistico è positivo o negativo.

Ma raramente i media offrono un contesto per i dati. La storia è stata pubblicata a seguito di un incidente in cui un bambino è stato involontariamente soffocato durante il sonno.

Ah, e quella statistica dei 20 neonati all'anno vale solo per il Minnesota. Nulla si dice se la situazione in altri stati è migliore o peggiore.

Il titolo nella versione Web dell'articolo è diverso.

<<http://www.startribune.com/local/49985722.html?elr=KArksUUUoDEy3LGDiO7aiU>>  
oppure <<http://tinyurl.com/nfzqcl>>

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

Frode su eBay

Mi aspettavo che vendere il mio computer su eBay fosse semplice.

Tentativo N. 1: L'ho messo in vendita. Nel giro di qualche ora, qualcuno lo ha acquistato -- da un account hackerato, come poi mi ha notificato eBay annullando la vendita.

Tentativo N. 2: L'ho messo in vendita di nuovo. Nel giro di qualche ora, qualcuno lo ha acquistato, e mi ha chiesto di inviarlo via FedEx overnight. Il compratore ha inviato immediatamente il pagamento via PayPal e poi, altrettanto rapidamente, ha aperto una disputa con PayPal in modo da sospendere il bonifico. Poi mi ha inviato un'email dicendomi "Io l'ho pagata, adesso mi deve spedire il computer". Ma immagino che PayPal sia stata più rapida del previsto, perché allo stesso tempo ho ricevuto un'email da PayPal che mi informava che era possibile che avessi ricevuto un pagamento non autorizzato dal titolare dell'account, e che non avrei dovuto spedire il computer prima che l'indagine in corso fosse terminata.

Stavo per compiere il Tentativo N. 3, ma un lettore del mio blog lo ha comprato prima. Pare che il sistema di eBay sia del tutto inefficace per oggetti di questo genere.

E non è capitato solo a me.

<<http://consumerist.com/5007790/its-now-completely-impossible-to-sell-a-laptop-on-ebay>>

oppure <<http://tinyurl.com/55hprp>>

Una copia di questo articolo, con i rimandi integrati nel testo, è disponibile sul mio blog:  
<[http://www.schneier.com/blog/archives/2009/06/fraud\\_on\\_ebay.html](http://www.schneier.com/blog/archives/2009/06/fraud_on_ebay.html)>

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

News

È stato un post pubblico su Twitter a portare a un furto con scasso?

<[http://www.usatoday.com/travel/news/2009-06-08-twitter-vacation\\_N.htm](http://www.usatoday.com/travel/news/2009-06-08-twitter-vacation_N.htm)>

Un gruppo di cani della prateria porta scompiglio al Baltimore Zoo; una storia divertente che richiama molti dei nostri problemi di sicurezza.

<<http://www.baltimoresun.com/news/maryland/baltimore-city/bal-md.ci.zoo12jun12,0,685569.story>>

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

Il Dipartimento per la Sicurezza Nazionale statunitense ha un blog. Non so se sarà interessante o divertente come quello della TSA:

<<http://www.dhs.gov/journal/theblog>>

In Svezia, un progetto artistico con finte 'carote-bomba' causa allarme:

<<http://news.bbc.co.uk/2/hi/europe/8099561.stm>>

Affascinante ricerca sulla psicologia dei raggiri. "The psychology of scams: Provoking and committing errors of judgement" (La psicologia delle truffe: provocare e commettere errori di valutazione) è stata preparata per l'Office of Fair Trading (Ministero per l'equità nei rapporti commerciali) del Regno Unito a opera della University of Exeter School of Psychology.

<[http://www.schneier.com/blog/archives/2009/06/the\\_psychology\\_3.html](http://www.schneier.com/blog/archives/2009/06/the_psychology_3.html)>

Un nuovo strumento informatico per spiare:

<<http://investors.guidancesoftware.com/releasedetail.cfm?ReleaseID=384544>>

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

La minaccia da trama cinematografica di questa settimana: funghi.

<[http://www.schneier.com/blog/archives/2009/06/this\\_weeks\\_movi.html](http://www.schneier.com/blog/archives/2009/06/this_weeks_movi.html)>

Gli ingegneri hanno più probabilità di trasformarsi in terroristi islamici. Almeno, questo è quanto indicano i fatti. È forse arrivato il momento di iniziare a effettuare il profiling?

<<http://www.newscientist.com/article/mg20227127.200-can-university-subjects-reveal-terrorists-in-the-making.html>>

oppure <<http://tinyurl.com/m5r56h>>

<<http://www.nuff.ox.ac.uk/users/gambetta/Engineers%20of%20Jihad.pdf>>

John Mueller sul disarmo nucleare: "L'idea per cui il mondo dovrebbe disfarsi delle armi nucleari è in circolazione da più di sessant'anni: in quest'arco di tempo sono state praticamente l'unico strumento di distruzione che non ha ucciso nessuno".

<[http://www.schneier.com/blog/archives/2009/06/john\\_mueller\\_on.html](http://www.schneier.com/blog/archives/2009/06/john_mueller_on.html)>

Intercettare le stampanti a matrice di punti ascoltandone il rumore.

<[http://www.schneier.com/blog/archives/2009/06/eavesdropping\\_o\\_3.html](http://www.schneier.com/blog/archives/2009/06/eavesdropping_o_3.html)>

Una ricerca sulla sicurezza dei giochi online:

<[http://www.schneier.com/blog/archives/2009/06/research\\_on\\_the.html](http://www.schneier.com/blog/archives/2009/06/research_on_the.html)>

Ross Anderson ha fatto il liveblogging dell'ottavo Workshop on Economics of Information Security (WEIS) alla University College London.

<<http://www.lightbluetouchpaper.org/2009/06/24/weis-2009-liveblog/>>

Ho parlato del WEIS 2006 nel 2006.

<[http://www.schneier.com/blog/archives/2006/06/economics\\_and\\_i\\_1.html](http://www.schneier.com/blog/archives/2006/06/economics_and_i_1.html)>

Clear, l'azienda che creò la corsia preferenziale ai checkpoint di sicurezza negli aeroporti, ha cessato l'attività. Non è chiaro che ne sarà di tutte le informazioni personali che ha raccolto finora.

<[http://www.schneier.com/blog/archives/2009/06/clear\\_shuts\\_dow.html](http://www.schneier.com/blog/archives/2009/06/clear_shuts_dow.html)>

Questo coltello senza punta non sembra uno scherzo.

<<http://www.timesonline.co.uk/tol/news/uk/crime/article6501720.ece>>

Ho già trattato dei rischi dei coltelli appuntiti.

<[http://www.schneier.com/blog/archives/2005/06/risks\\_of\\_pointy.html](http://www.schneier.com/blog/archives/2005/06/risks_of_pointy.html)>

Il Communication Security Establishment (CSE, in sostanza l'equivalente canadese della NSA) sta crescendo a una tale velocità che non ha più spazio nell'attuale edificio e ne sta costruendo altri.

<<http://www.defenseindustrydaily.com/Canadas-CSE-ELINT-Agency-Building-New-Facilities-05498/>>

oppure <<http://tinyurl.com/leu79h>>

Spam crittografico:

<[http://www.schneier.com/blog/archives/2009/06/cryptography\\_sp.html](http://www.schneier.com/blog/archives/2009/06/cryptography_sp.html)>

Altre misure di sicurezza dal mondo della natura:

1. La pianta *caladium steudneriifolium* finge di essere malata così non verrà divorata dalle larve di insetti fitofagi.

<[http://news.bbc.co.uk/earth/hi/earth\\_news/newsid\\_8108000/8108940.stm](http://news.bbc.co.uk/earth/hi/earth_news/newsid_8108000/8108940.stm)>

2. Gli afidi giallastri delle Ombrellifere si armano di bombe chimiche.

<[http://scienceblogs.com/notrocketscience/2009/06/aphids\\_defend\\_themselves\\_with\\_chemical\\_bombs.php](http://scienceblogs.com/notrocketscience/2009/06/aphids_defend_themselves_with_chemical_bombs.php)>

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

3. Il ragno-formica dalle zampe scure imita una formica, così non viene mangiato da altri ragni e può cacciarli a sua volta.

<[http://scienceblogs.com/notrocketscience/2009/06/spiders\\_gather\\_in\\_groups\\_to\\_impersonate\\_ants.php](http://scienceblogs.com/notrocketscience/2009/06/spiders_gather_in_groups_to_impersonate_ants.php)>

oppure <<http://tinyurl.com/p9u8r9>>

<[http://scienceblogs.com/notrocketscience/2009/07/spider\\_mimics\\_ant\\_to\\_eat\\_spiders\\_and\\_avoid\\_being\\_eaten\\_by\\_spiders.php](http://scienceblogs.com/notrocketscience/2009/07/spider_mimics_ant_to_eat_spiders_and_avoid_being_eaten_by_spiders.php)>

oppure <<http://tinyurl.com/mhjxh3>>

Tastierini numerici che divulgano involontariamente informazioni. (Bisogna fare clic sul link per vedere le immagini)

<[http://www.schneier.com/blog/archives/2009/07/information\\_lea\\_1.html](http://www.schneier.com/blog/archives/2009/07/information_lea_1.html)>

Un buon articolo -- "The Staggering Cost of Playing it 'Safe'" (L'incredibile costo di 'andare sul sicuro') -- sulle motivazioni politiche alla base della condotta di sicurezza dei terroristi.

<<http://www.dailykos.com/storyonly/2009/6/16/743102/-The-Staggering-Cost-of-Playing-it-Safe>>

oppure <<http://tinyurl.com/m8dlvr>>

Un mio commento a un articolo che esalta i rischi terroristici del cloud computing:

<[http://www.schneier.com/blog/archives/2009/07/terrorist\\_risk.html](http://www.schneier.com/blog/archives/2009/07/terrorist_risk.html)>

Pantaloni senza tasche per difendersi dalla corruzione in Nepal:

<<http://www.google.com/hostednews/afp/article/ALeqM5gmKIu2qKjavgL6B0s7161VCyMSAQ>>

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

Sacchetti per il pranzo... antifurto:

<<http://design-milk.com/anti-theft-lunch-bags/>>

Un tribunale statunitense stabilisce dei limiti alle perquisizioni della TSA. Un'ottima notizia.

<[http://www.schneier.com/blog/archives/2009/07/court\\_limits\\_on.html](http://www.schneier.com/blog/archives/2009/07/court_limits_on.html)>

La polizia spagnola Spanish sventa un piano di evasione che comprendeva un piccolo zeppelin radiocomandato. A volte le trame cinematografiche accadono davvero.

<<http://gizmodo.com/5307943/spanish-police-foil-remote+controlled-zeppelin-jailbreak>>

oppure <<http://tinyurl.com/qcns4y>>

<<http://www.thestar.com/news/world/article/660875>>

Circa due anni fa, scrissi della mia strategia per criptare il mio portatile. Fra le altre cose, dissi: "Tuttavia esistono ancora due scenari contro i quali non si è protetti. Non siete protetti nel caso qualcuno vi rubi il portatile di mano mentre state scrivendo qualcosa seduti in un caffè; e non siete protetti nel caso le autorità vi chiedano di togliere la criptatura dai vostri dati". Ecco un programma gratuito che vi protegge dalla prima minaccia: blocca il computer a meno che un tasto non venga premuto ogni n secondi. Onestamente per me sarebbe troppo fastidioso da usare, ma potete provarlo.

<<http://www.donationcoder.com/Forums/bb/index.php?topic=18656.0>>

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

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

Non sentirete parlare di questa vulnerabilità dei bancomat perché la presentazione è stata ritirata dalla BlackHat conference:

<[http://www.schneier.com/blog/archives/2009/07/the\\_atm\\_vulnera.html](http://www.schneier.com/blog/archives/2009/07/the_atm_vulnera.html)>

La NSA sta costruendo un gigantesco data center nello Utah.

<[http://www.sltrib.com/ci\\_12735293](http://www.sltrib.com/ci_12735293)>

<<http://www.deseretnews.com/article/705314456/Psst-Big-spy-center-is-coming-to-Utah.html>>

oppure <<http://tinyurl.com/nrn64r>>

Sono stato citato definendo Google Chrome OS "idiota". Ecco una spiegazione più approfondita e un po' di contesto.

<[http://www.schneier.com/blog/archives/2009/07/making\\_an\\_opera.html](http://www.schneier.com/blog/archives/2009/07/making_an_opera.html)>

Come provocare il caos in un aeroporto: lasciare una valigetta nelle toilette.

<[http://www.schneier.com/blog/archives/2009/07/lost\\_suitcases.html](http://www.schneier.com/blog/archives/2009/07/lost_suitcases.html)>

Uno studio interessante da HotSec '07: "Do Strong Web Passwords Accomplish Anything?" (Le password forti usate nel Web servono a qualcosa?) di Dinei Florencio, Cormac Herley e Baris Coskun.

<[http://www.usenix.org/event/hotsec07/tech/full\\_papers/florencio/florencio.pdf](http://www.usenix.org/event/hotsec07/tech/full_papers/florencio/florencio.pdf)>

oppure <<http://tinyurl.com/ca9mp9>>

Interessante utilizzo di software per la rilevazione dello sguardo allo scopo di proteggere la privacy:

<[http://www.schneier.com/blog/archives/2009/07/gaze\\_tracking\\_s.html](http://www.schneier.com/blog/archives/2009/07/gaze_tracking_s.html)>

Steganografia dei poveri: nascondere documenti in file PDF corrotti.

<<http://blog.didierstevens.com/2009/07/01/embedding-and-hiding-files-in-pdf-documents/>>

oppure <<http://tinyurl.com/m6onbo>>

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

Autenticare i documenti cartacei

È una storia triste e tremenda. Un uomo torna a casa e scopre che è stata demolita. L'impresa di demolizioni è stata assunta regolarmente, ma c'è stato un errore e ha demolito la casa sbagliata. L'impresa di demolizioni si è affidata alle coordinate GPS, ma richiedere l'indirizzo non è una soluzione -- un errore di stampa nell'indirizzo sarebbe stato altrettanto probabile, e avrebbe portato a una altrettanto rapida demolizione della casa.

Il problema non risiede tanto nel come i demolitori sapevano quale casa distruggere, ma nel come hanno verificato le informazioni. Si sono fidati della documentazione cartacea, e tale documentazione era scorretta. L'informalità funziona quando tutti si conoscono fra loro. Quando i commercianti e i cittadini si conoscono, quando ufficiali governativi e cittadini si conoscono, e ognuno conosce i propri vicini, la gente sa che cosa succede. In quel genere di ambiente se qualcosa va storto non passa inosservato.

Nel nostro mondo moderno e anonimo, la documentazione cartacea è quel che fa andare avanti le cose. Tradizionalmente le firme, i moduli e le filigrane rendevano ufficiale un documento. Le falsificazioni erano possibili, ma difficili da realizzare. Oggi la documentazione cartacea esiste ancora, ma per la maggior parte solo fino a quando le informazioni non raggiungono un database informatico. Nel frattempo la tecnologia moderna (computer, fax e software per il desktop publishing) hanno facilitato di molto il procedimento di falsificazione dei documenti. Ogni caso di furto di identità ha, al suo centro, un errore a livello di documentazione. Ordini di lavoro, ordini di acquisto, e altri documenti fasulli vengono utilizzati per rubare computer, attrezzature e merci. Di tanto in tanto, grazie a un fax falso qualcuno riesce a uscire di prigione. Carte d'imbarco fasulle permettono di passare la sicurezza aeroportuale. Questo mese degli hacker hanno cambiato ufficialmente il nome di un uomo svedese.

Un reporter è persino riuscito ad attestarsi la proprietà dell'Empire State Building. Certo, è stato uno scherzo, ma si tratta di una forma di reato in crescita. Qualcuno finge di essere voi (preferibilmente quando siete in vacanza) e vende la vostra casa a qualcun altro, falsificando il vostro nome sui documenti. Voi tornate e trovate un estraneo in casa vostra, qualcuno che crede di averla legittimamente acquistata. In un certo senso non è una novità. Errori e frodi con i documenti sono sempre successi, sin da quando esistono i documenti. E il problema non è ancora stato risolto per tutta una serie di ragioni.

Uno: i nostri sistemi imprecisi e trascurati in genere funzionano bene, ed è così che tiriamo avanti con il minimo sforzo. La maggioranza delle case non vengono demolite per sbaglio e la maggioranza delle persone non si ritrovano con il nome cambiato da dei malviventi. Per comune che sia il furto di identità, non capita alla maggior parte di noi. Queste storie fanno notizia perché sono così rare. E i molti casi costa meno pagare per un errore che assicurarsi che non accada mai.

Due: a volte mancano gli incentivi affinché la documentazione sia autenticata in maniera appropriata. Le persone che hanno demolito quella casa stavano semplicemente facendo il proprio lavoro. Stesso dicasi per i funzionari governativi addetti al cambio di nome e titolo. Le banche vengono pagate quando il denaro viene trasferito da un conto all'altro, non quando incontrano un problema nei documenti. Tutti siamo irritati da moduli timbrati 17 volte e da altri misteriosi procedimenti burocratici, ma in realtà questi processi sono ideati per rilevare eventuali problemi.

Tre: vi è una discrepanza psicologica: è facile falsificare i documenti, eppure nella maggior parte dei casi agiamo come se la documentazione avesse poteri magici di autenticità.

Ciò che è cambiato è la scala, l'ordine di grandezza. Una frode può venire perpetrata automaticamente ai danni di centinaia di migliaia di persone. Anche dei banali errori possono colpire un numero così grande di malcapitati. Abbiamo bisogno di leggi che puniscano individui o aziende -- penalmente o civilmente -- che commettono errori di documentazione. Questo fa innalzare il costo degli sbagli, e rende l'autenticazione dei documenti una strada più appetibile, il che cambia gli incentivi delle parti che ricevono la documentazione. E tutto questo farà sì che il mercato studierà delle tecnologie per verificare la provenienza, l'esattezza e l'integrità delle informazioni: verifiche telefoniche, indirizzi e coordinate GPS, autenticazione crittografica, sistemi che effettuano controlli doppi e tripli, e via dicendo.

Non possiamo ridurre la dipendenza della società dai documenti, e non possiamo eliminare gli errori da essi generati. Ma possiamo instaurare degli incentivi economici che spingano i privati e le aziende ad autenticare la documentazione maggiormente e in modo migliore.

Questo articolo è originariamente apparso sul Guardian.  
<<http://www.guardian.co.uk/technology/2009/jun/24/read-me-first-identity-fraud>>  
oppure <<http://tinyurl.com/l3cdp>>

Rimandi:

<<http://www.wsbtv.com/news/19715994/detail.html>>  
<[http://www.schneier.com/blog/archives/2008/06/fax\\_signatures\\_1.html](http://www.schneier.com/blog/archives/2008/06/fax_signatures_1.html)>  
<[http://www.schneier.com/blog/archives/2006/11/forge\\_your\\_own.html](http://www.schneier.com/blog/archives/2006/11/forge_your_own.html)>  
<<http://torrentfreak.com/pirate-bay-nemesis-has-name-changed-by-pranksters-090607/>>  
<[http://www.schneier.com/blog/archives/2008/12/how\\_to\\_steal\\_th.html](http://www.schneier.com/blog/archives/2008/12/how_to_steal_th.html)>  
<[http://www.schneier.com/blog/archives/2006/09/land\\_title\\_frau.html](http://www.schneier.com/blog/archives/2006/09/land_title_frau.html)>  
<[http://www.schneier.com/blog/archives/2005/08/identity\\_thief.html](http://www.schneier.com/blog/archives/2005/08/identity_thief.html)>

Una copia di questo articolo, con i rimandi integrati nel testo, è disponibile sul mio blog:  
<[http://www.schneier.com/blog/archives/2009/06/authenticating\\_1.html](http://www.schneier.com/blog/archives/2009/06/authenticating_1.html)>

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

I pro e i contro del mascheramento della password

Jakob Nielsen, guru dell'usabilità, ha scatenato un polverone quando sul suo blog si è dichiarato contrario al mascheramento della password, ossia la pratica di nascondere dietro asterischi le lettere che formano una password. Sono intervenuto dicendo di essere d'accordo. Dopo più di 165 commenti sul mio blog, svariati articoli, saggi e molti altri interventi su altri blog, secondo l'opinione generale Nielsen e io avevamo torto.

Ammetto di essere stato un po' facilone. Come ogni misura di sicurezza, il mascheramento della password ha un valore. Ma come ogni misura di sicurezza, il mascheramento della password non è una panacea. E occorre bilanciarne i costi e i benefici.

Il costo è l'accuratezza. Quando gli utenti non ricevono un feedback visivo di ciò che stanno digitando, sono maggiormente soggetti a errori. Questo vale specialmente nel caso di stringhe che presentano caratteri non standard e un misto di lettere maiuscole e minuscole. Ciò porta ad altri costi secondari:

- \* Gli utenti si arrabbiano.

- \* Gli utenti saranno più propensi a scegliere password semplici da inserire, riducendo così sia gli errori che la sicurezza. Eliminare il mascheramento della password metterà le persone a proprio agio con password complicate: diventeranno più facili da ricordare e da impiegare.

I benefici del mascheramento della password sono più evidenti:

- \* Protezione dal cosiddetto 'shoulder surfing' (cioè sbirciare alle spalle). Se gli altri non possono sbirciare alle nostre spalle e vedere che cosa stiamo scrivendo, sarà più difficile che riescano a sottrarci la password. Sì, potrebbero osservare le nostre dita, ma è ancora più arduo che cercare di guardare lo schermo. Anche le telecamere di sorveglianza sono un problema: è più facile osservare i movimenti delle dita su una registrazione video, ma leggere una password in chiaro dallo schermo che viene filmato è banale.

- \* In alcune situazioni scatta una dinamica di fiducia. Voi immettete la vostra password mentre il vostro capo sta in piedi dietro di voi e osserva quel che state facendo? O il vostro coniuge o partner? O un genitore o un figlio? O il vostro insegnante o i vostri studenti? Agli sportelli bancomat esiste la convenzione sociale di mantenere una certa distanza dalla persona che sta utilizzando il bancomat, ma tale convenzione non viene applicata ai computer. Potreste non fidarvi abbastanza della persona che vi sta accanto e non volere che veda la vostra password, e al tempo stesso il dover dire a questa persona di guardare altrove potrebbe farvi sentire a disagio. Il mascheramento della password risolve l'imbarazzo della situazione.

- \* Protezione dal malware che analizza le schermate. Questo è un problema minore, in quanto i keyboard logger sono più diffusi e non vengono fermati dal mascheramento della password. E se vi trovate con quel tipo di malware sul vostro computer, allora i problemi sono ben altri.

- \* Un 'segnale' di sicurezza. Il mascheramento della password avverte gli utenti, specie quelli poco pratici di sicurezza, che le password sono un segreto.

Ritengo che lo shoulder surfing sia un problema meno grosso di quanto si dica. In primo luogo, moltissime persone utilizzano i loro computer in privato, e nessuno in quel caso sta in piedi dietro di loro a sbirciare. Secondariamente, i dispositivi palmari personali vengono utilizzati molto vicino al corpo, rendendo molto arduo spiare da dietro le spalle. In terzo luogo è difficile memorizzare rapidamente e precisamente una stringa casuale non alfanumerica che appare a video per un secondo o poco più.

Con questo non intendo dire che lo shoulder surfing non sia una minaccia: lo è. E, come hanno fatto notare molti lettori, il mascheramento della password è uno dei motivi per cui lo shoulder surfing è meno pericoloso. E i rischi sono maggiori per quegli utenti poco pratici con i computer: persone lente a digitare e persone con la tendenza a scegliere password mediocri. Ma credo che i rischi siano sopravvalutati.

Il mascheramento della password è assolutamente importante sui terminali pubblici con PIN corti (come i bancomat). Il valore del PIN è più grande, lo shoulder surfing è più comune, e un PIN a quattro cifre è comunque molto facile da ricordare.

E infine questo problema sparisce in gran parte su Internet sul vostro computer. Moltissimi browser comprendono la possibilità di salvare e poi riempire automaticamente i campi delle password, eliminando così l'inconveniente dell'usabilità a scapito però di un altro problema di sicurezza (la sicurezza della password diventa la sicurezza del computer). Esiste un plug-in per Firefox che elimina il mascheramento della password. E programmi come il mio Password Safe permettono di tagliare e incollare le password nelle applicazioni, anche qui risolvendo il problema dell'usabilità.

Un'alternativa è rendere il mascheramento un'opzione configurabile. Applicazioni di banking ad alto rischio potrebbero attivare il mascheramento della password per default; altre applicazioni potrebbero disattivarlo per default. I browser in luoghi pubblici potrebbero attivarlo per default, eccetera. Mi piace questa soluzione, ma complica l'interfaccia utente.

Un lettore ha accennato alla soluzione di BlackBerry e di iPhone, ossia visualizzare ogni carattere della password per un breve istante prima di mascherarlo. Mi sembra un compromesso eccellente.

A me piacerebbe questa opzione. Non riesco a digitare chiavi WEP complesse in Windows -- e per due volte! Ma perché, poi? -- senza fare errori. Non riesco a immettere le mie chiavi PGP (che uso raramente e che sono parecchio complicate) senza fare errori a meno di non disattivare il mascheramento della password. Ecco a cosa stavo reagendo quando ho detto a Nielsen "Sono d'accordo".

E quindi avevo torto? Forse. Okay, probabilmente. Il mascheramento della password migliora certamente la sicurezza; molti lettori hanno detto di utilizzare i loro computer in ambienti affollati, e si affidano al mascheramento per proteggere le loro password. D'altra parte il mascheramento della password riduce la precisione e fa in modo che gli utenti siano meno propensi a scegliere password sicure, forti e difficili da ricordare. Ammetto che il compromesso del mascheramento è molto più vantaggioso di quanto avessi inizialmente pensato con la mia reazione impulsiva, ma anche che la risposta non è così ovvia come abbiamo sempre storicamente assunto.

Rimandi:

<<http://www.useit.com/alertbox/passwords.html>>

<[http://www.schneier.com/blog/archives/2009/06/the\\_problem\\_wit\\_2.html](http://www.schneier.com/blog/archives/2009/06/the_problem_wit_2.html)>  
<[http://www.schneier.com/blog/archives/2009/06/the\\_problem\\_wit\\_2.html#comments](http://www.schneier.com/blog/archives/2009/06/the_problem_wit_2.html#comments)>  
<<http://www.thetechherald.com/article.php/200926/3949/Is-usability-worth-more-than-security>>  
<<http://www.out-law.com/page-10128>>  
<<http://www.cgisecurity.com/2009/06/masked-passwords-must-go.html>>  
<<http://countermeasures.trendmicro.eu/password-masking-a-necessary-evil/>>  
<<http://blog.securityactive.co.uk/2009/07/01/apparently-we-should-no-longer-blank-passwords-when-entered-on-websites-thoughts/>>  
<<http://www.jahne.com/information-and-removal/about-face-on-bruce-schneier/>>  
<<http://usabilityprinciples.edublogs.org/2009/07/01/to-oppure-not-to-mask-usability-versus-security-in-password-masking-malware-blog-trend-micro/>>  
<<http://www.schneier.com/passsafe.html>>

Una copia di questo articolo, con i rimandi integrati nel testo, è disponibile sul mio blog:  
<[http://www.schneier.com/blog/archives/2009/07/the\\_pros\\_and\\_co.html](http://www.schneier.com/blog/archives/2009/07/the_pros_and_co.html)>

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

## I "costi occulti" della privacy

Forbes ha pubblicato un articolo sui costi 'occulti' della privacy. Fondamentalmente, il punto è che è costoso conformarsi alle regolamentazioni sulla privacy, e una buona fetta di tale spesa viene assorbita dai meccanismi di conformità e non serve al miglioramento effettivo della privacy di nessuno. Questo è un punto valido, che ripeto in continuazione ogni volta che parlo della privacy in pubblico. È una situazione particolarmente grave negli Stati Uniti, perché abbiamo un mosaico di diverse leggi sulla privacy che coprono i diversi tipi di informazioni e di situazioni, e non abbiamo un'unica legge onnicomprensiva sulla privacy.

I meta-problema è semplice da descrivere: le entità a cui affidiamo la nostra privacy spesso non hanno grandi incentivi per rispettarla. Esempi: agenzie di credito, come Experian e TransUnion, che non hanno alcun rapporto d'affari diretto con le persone i cui dati raccolgono e rivendono; società come Google che 'regalano' servizi -- e raccolgono informazioni personali come parte del rapporto -- come incentivo per visionare annunci pubblicitari, e fare i soldi con la vendita di tali annunci ad altre società; imprese di assicurazione medica, che sono scelte dal datore di lavoro di una persona; e fornitori di software per computer, che possono avere poteri di monopolio sul mercato. Ancora peggio, può essere impossibile collegare un effetto di una violazione della privacy con la violazione stessa -- se qualcuno apre un conto bancario a vostro nome, come si fa a sapere chi è la colpa per la violazione della privacy? -- e perciò anche quando vi è un rapporto d'affari, la relazione causa-effetto non è altrettanto chiara.

Quel che significa tutto questo è che la protezione della privacy del singolo rimane un eternalità per molte aziende, e che le dinamiche di mercato basilari non potranno risolvere il problema. Dato che la soluzione di mercato efficiente non funziona, ecco che ci ritroviamo con soluzioni di regolamentazione inefficienti. Quindi ora la domanda

diventa: come si fa a rendere la normativa il più efficiente possibile? Ho alcuni suggerimenti:

- \* Regolamentazioni di privacy ad ampio respiro sono migliori di regolamentazioni ristrette.
- \* Meglio regolamentazioni semplici e chiare che complesse e disorientanti.
- \* È molto meglio regolamentare i risultati che non la metodologia.
- \* Le sanzioni per un comportamento scorretto devono essere sufficientemente costose da far diventare la condotta corretta la scelta più razionale.

Non ci sbarazzeremo mai delle inefficienze di regolamentazione - è la natura della bestia, e il motivo per cui una normativa ha senso solo quando il mercato fallisce - ma possiamo ridurle.

L'articolo di Forbes:

<<http://www.forbes.com/forbes/2009/0608/034-privacy-research-hidden-cost-of-privacy.html>>

oppure <<http://tinyurl.com/obpf6j>>

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

Sistemare la sicurezza aeroportuale

Sono mesi che la TSA (Transportation Security Administration) non ha un direttore fisso. Se, in un ipotetico colloquio di lavoro, il presidente Obama mi domandasse come sistemerei la sicurezza aeroportuale in una frase, risponderei: "Sbarazziamoci del controllo dei documenti con foto, e ripristiniamo lo screening dei passeggeri ai livelli anteriori all'11 settembre".

D'accordo, sto scherzando. Malgrado il mostrare un documento, il togliersi le scarpe e il gettar via bottigliette d'acqua non siano misure che ci rendono molto più sicuri, non mi aspetto che l'amministrazione Obama faccia dietrofront su queste misure di sicurezza tanto presto. La sicurezza negli aeroporti è più che altro per pararsi le spalle, e ci difende contro quel che i terroristi hanno tentato l'ultima volta.

Ma l'amministrazione non può rischiare di apparire come se stesse facilitando un attacco terroristico, non importa quanto remota sia la possibilità, per cui quelle seccature di cui sopra saranno probabilmente destinate a rimanere.

La mia vera risposta sarebbe questa: "Stabilire responsabilità e trasparenza per lo screening negli aeroporti". E se avessi un'altra frase a disposizione: "Gli aeroporti sono uno di quei luoghi in cui gli americani e chi viene a visitare l'America hanno la maggiore probabilità di interagire con un agente delle forze dell'ordine; eppure nessuno sa quali siano i diritti dei viaggiatori né come esercitarli".

Obama ha più volte parlato di aumentare l'apertura e la trasparenza al governo, ed è ora di portare la trasparenza alla Transportation Security Administration (TSA).

Cominciamo dalle watch list e dalle no-fly list. Allo stato attuale, tutto ciò che le riguarda è segreto: non potete sapere se vi trovate in una di esse, o chi vi ci ha messo e perché, e non potete togliere il vostro nome se siete innocenti. Questo scenario kafkiano è così non-americano da essere imbarazzante. Obama dovrebbe sottoporre la no-fly list a una revisione giudiziaria.

Poi veniamo ai checkpoint di sicurezza medesimi. Quali sono i nostri diritti? Quali poteri hanno gli agenti della TSA? Se ci vengono fatte delle domande 'amichevoli' da agenti addetti al rilevamento comportamentale, che cosa ci è permesso non rispondere? Se avanziamo rimostranze per il brusco trattamento a cui noi o i nostri bagagli sono stati sottoposti, può l'agente della TSA rivalersi contro di noi mettendoci in una watch list? Obama dovrebbe rendere le norme chiare ed esplicite, e permettere alle persone di agire legalmente contro la TSA in caso di violazioni; altrimenti i checkpoint negli aeroporti rimarranno una zona senza Costituzione nel nostro paese.

Poi Obama dovrebbe rifiutarsi di utilizzare mandati non consolidati per far passare costose misure di sicurezza aggirando il Congresso. Il programma Secure Flight è il peggior esempio in questo senso. Le linee aeree sono costrette a spendere miliardi di dollari per rivedere i propri sistemi di prenotazione così da venire incontro alle pretese della TSA di pre-approvare ogni passeggero prima che la persona sia autorizzata a imbarcarsi. Questi costi vengono sostenuti dai contribuenti, sotto forma di prezzi del biglietto più elevati, anche se non sono mai esplicitamente indicati.

Forse Secure Flight è un buon sistema per utilizzare il nostro denaro; forse non lo è. Ma perché non portiamo il dibattito allo scoperto, come parte del processo di budget, come è giusto che sia?

E infine, Obama dovrebbe ordinare che la sicurezza aeroportuale riguardi soltanto il terrorismo, e che non serva come checkpoint di sicurezza a tutto campo per beccare chiunque, da ragazzi che fumano marijuana a padri fannulloni.

La Costituzione offre sia ai cittadini americani che ai visitatori una serie di protezioni forti contro perquisizioni di polizia troppo invadenti. Ai checkpoint di sicurezza negli aeroporti vi sono due eccezioni. La prima si chiama 'implied consent' (consenso implicito), e significa che non si può rifiutare la perquisizione; il consenso viene dato implicitamente con l'acquisto del biglietto. La seconda si chiama 'plain view' (in piena vista), e significa che se l'agente della TSA nota qualcosa che non ha nulla a che vedere con la sicurezza aeroportuale mentre vi sta controllando, gli è permesso agire di conseguenza.

Entrambi questi principi sono ormai ben riconosciuti e hanno senso, ma è la loro combinazione che trasforma i checkpoint di sicurezza negli aeroporti in checkpoint da stato di polizia.

La TSA dovrebbe limitare le perquisizioni, concentrandosi su bombe e armi, e lasciare il lavoro di polizia alle forze dell'ordine, nel cui ambito sappiamo di poterci avvalere di tribunali e della Costituzione.

Nessuno di questi cambiamenti renderà gli aeroporti meno sicuri, ma contribuiranno decisamente a depotenziare la cultura del terrore, ripristinando la presunzione di innocenza e rassicurando gli americani e il resto del mondo che, come ha detto Obama

nel suo discorso inaugurale, "respingiamo come falsa la scelta fra la nostra sicurezza e i nostri ideali".

Rimandi:

<[http://www.schneier.com/blog/archives/2007/02/cya\\_security\\_1.html](http://www.schneier.com/blog/archives/2007/02/cya_security_1.html)>  
<[http://www.whitehouse.gov/the\\_press\\_office/TransparencyandOpenGovernment/](http://www.whitehouse.gov/the_press_office/TransparencyandOpenGovernment/)>  
<<http://www.eff.org/files/filenode/foia/2009foia.mem.rel.pdf>>  
<<http://www.schneier.com/essay-052.html>>  
<[http://www.usatoday.com/travel/columnist/grossman/2009-06-02-secure-flight\\_N.htm](http://www.usatoday.com/travel/columnist/grossman/2009-06-02-secure-flight_N.htm)>  
<[http://www.tsa.gov/press/happenings/florida\\_uniform.shtm](http://www.tsa.gov/press/happenings/florida_uniform.shtm)>  
<<http://www.washingtonpost.com/wp-dyn/articles/A33132-2004Aug1.html>>  
<[http://media.washingtonpost.com/wp-srv/politics/documents/Obama\\_Inaugural\\_Address\\_012009.html](http://media.washingtonpost.com/wp-srv/politics/documents/Obama_Inaugural_Address_012009.html)>

Questo articolo è originariamente apparso (senza link) nel New York Daily News.

<[http://www.nydailynews.com/opinions/2009/06/24/2009-06-24\\_clear\\_common\\_sense\\_for\\_takeoff\\_how\\_the\\_tsa\\_can\\_make\\_airport\\_security\\_work\\_for\\_pa.html](http://www.nydailynews.com/opinions/2009/06/24/2009-06-24_clear_common_sense_for_takeoff_how_the_tsa_can_make_airport_security_work_for_pa.html)>

oppure <<http://tinyurl.com/kwa2pd>>

<[http://www.schneier.com/blog/archives/2009/06/fixing\\_airport.html](http://www.schneier.com/blog/archives/2009/06/fixing_airport.html)>

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

Le news su Schneier

Interverrò alla Black Hat and DefCon, a Las Vegas, il 30 e 31 luglio 2009.

<https://www.blackhat.com/html/bh-usa-09/bh-us-09-main.html>

<<http://defcon.org/html/defcon-17/dc-17-index.html>>

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

Una svolta nell'ambito della crittografia omomorfica

Il mese scorso IBM ha rilasciato alcune dichiarazioni piuttosto chiosose in merito alla crittografia omomorfica e al futuro della sicurezza. Mi spiace fare la parte di chi spegne gli entusiasmi, malgrado la nuova scoperta sia indubbiamente interessante, ma è importante separare la teoria dalla pratica.

I sistemi crittografici omomorfici sono quelli in cui le operazioni matematiche sul ciphertext (testo cifrato) hanno effetti regolari sul plaintext (testo in chiaro). Un normale algoritmo di crittografia simmetrico -- DES, AES, ecc. -- non è omomorfico. Assumiamo di avere il plaintext P e di criptarlo con AES per ottenere il ciphertext C corrispondente. Se moltiplichiamo quel ciphertext per 2, e poi decodifichiamo 2C, otterremo un pasticcio di caratteri casuali invece di P. Se ottenessimo qualcos'altro, come 2P per esempio, questo implicherebbe alcune proprietà di non casualità di AES piuttosto marcate, e nessuno si fiderebbe della sua sicurezza.

L'algoritmo RSA è diverso. Criptiamo P per ottenere C, moltiplichiamo C per 2, e poi decodifichiamo 2C, e otterremo 2P. Questo è un omomorfismo: si effettuino delle operazioni matematiche al ciphertext, e tali operazioni saranno riflesse nel plaintext. L'algoritmo RSA è omomorfo rispetto alla moltiplicazione, un fattore che deve essere tenuto in considerazione quando si valuta la sicurezza di un sistema di sicurezza che fa uso di RSA.

Fin qui nulla di nuovo. L'omomorfismo di RSA è noto sin dagli anni Settanta, e altri algoritmi che sono omomorfi rispetto all'addizione si conoscono dagli anni Ottanta. Ma quel che è sfuggito ai crittografi è un sistema crittografico pienamente omomorfo: ovvero omomorfo sia rispetto all'addizione che alla moltiplicazione, e al tempo stesso conserva la propria sicurezza. Ed è quel che ha scoperto un ricercatore di IBM, Craig Gentry.

È qualcosa di molto più importante di quanto possa apparire a prima vista. Qualunque calcolo può venire espresso come un circuito booleano: una serie di addizioni e moltiplicazioni. Il nostro computer è costituito da un fantastilione di circuiti booleani, ed è possibile eseguire programmi che facciano qualsiasi cosa. Questo algoritmo significa poter effettuare calcoli arbitrari su dati criptati omomorficamente. Più concretamente: se criptiamo dati in un sistema crittografico pienamente omomorfo, possiamo passare quei dati a una persona non fidata, e quella persona potrà effettuare calcoli arbitrari su quei dati senza poter decodificare i dati stessi. Immaginate che cosa significherebbe per il cloud computing, o per qualsiasi infrastruttura di outsourcing: non sarebbe più necessario affidare i dati all'outsourcer.

Purtroppo (sapevate che c'era un 'purtroppo' a questo punto, no?) lo schema di Gentry è tutt'altro che pratico. Utilizza una cosa chiamata reticolo ideale come base dello schema crittografico, e sia le dimensioni del ciphertext che la complessità delle operazioni di codifica e decodifica crescono enormemente con la quantità di operazioni che occorre effettuare sul ciphertext -- e tale quantità deve essere fissata in partenza. E convertire un programma, anche il più semplice, in un circuito booleano richiede un numero incredibile di operazioni. Queste non sono scomodità che si possono risolvere con qualche brillante tecnica di ottimizzazione e qualche giro della legge di Moore; si tratta di una limitazione intrinseca dell'algoritmo. In un articolo Gentry stima che l'esecuzione di una ricerca in Google utilizzando termini criptati (una semplice applicazione assolutamente plausibile di questo algoritmo) aumenterebbe il tempo di calcolo di circa un trilione di volte. Secondo la legge di Moore ci vorrebbero 40 anni prima che quella ricerca omomorfa diventasse efficiente come una ricerca attuale, e ritengo che Gentry sia ottimista persino con questo esempio semplicissimo.

Malgrado ciò, la macchina delle pubbliche relazioni di IBM è impazzita dopo la scoperta. Per come ne parla il comunicato stampa, sembrerebbe che questo nuovo schema omomorfo riscriverà l'intero business informatico: non solo il cloud computing, ma anche "l'attivazione di filtri antispam anche sulla posta criptata, o informazioni di protezione contenute nelle cartelle cliniche elettroniche". Un giorno magari, ma non nella mia epoca.

Con questo non voglio togliere nulla a Gentry o alla sua scoperta. Visioni di un sistema crittografico pienamente omomorfo hanno danzato nelle menti dei crittografi per un trentennio. Non mi sarei mai aspettato di vederne uno. Passeranno anni prima che un numero sufficiente di crittografi esaminerà l'algoritmo e potremo avere una qualche

certezza che lo schema sia davvero sicuro, ma -- praticità a parte -- questa scoperta è davvero impressionante.

Rimandi:

<<http://portal.acm.org/citation.cfm?doid=1536414.1536440>>  
<[http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=compliance&articleId=9134823&taxonomyId=152&intsrc=kc\\_top](http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=compliance&articleId=9134823&taxonomyId=152&intsrc=kc_top)>  
<<http://www.prnewswire.com/cgi-bin/stories.pl?ACCT=104&STORY=/www/story/06-25-2009/0005050200&EDATE=>>

Una copia di questo articolo, con i rimandi integrati nel testo, è disponibile sul mio blog:  
<[http://www.schneier.com/blog/archives/2009/07/homomorphic\\_enc.html](http://www.schneier.com/blog/archives/2009/07/homomorphic_enc.html)>

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

## Nuovo attacco contro AES

C'è un nuovo attacco crittanalitico contro AES che è migliore della forza bruta:

“Abstract. In questo studio presentiamo due attacchi related-key contro l'intero AES. Per AES-256 dimostriamo il primo attacco di key recovery, che funziona per tutte le chiavi e ha complessità  $2^{119}$ , mentre il recente attacco di Biryukov-Khovratovich-Nikolic funziona su una classe di chiavi debole e presenta una complessità maggiore. Il secondo attacco è la prima crittanalisi dell'intero AES-192. Entrambi i nostri attacchi sono attacchi boomerang, che si basano sull'idea recente di scoprire collisioni locali nei block cipher e sono potenziati grazie alle tecniche boomerang di switching in modo da ottenere round liberi nel mezzo”.

In una email, gli autori hanno scritto: “Ci aspettiamo anche che un'attenta analisi possa ridurre la complessità. Come risultato preliminare, riteniamo che la complessità dell'attacco contro AES.256 possa essere diminuita da  $2^{119}$  a circa  $2^{110,5}$  (dati e tempo). Crediamo che questi risultati possano gettare una nuova luce sul design dei key-schedule dei block cipher, ma non rappresentano alcuna minaccia per le applicazioni nel mondo reale che sfruttano l'algoritmo AES”.

Sono d'accordo. Se da un lato questo attacco è migliore della forza bruta (e per questo alcuni crittografi diranno che l'algoritmo è 'compromesso'), è ancora molto, molto al di là delle nostre capacità di calcolo. L'attacco è, e probabilmente sempre sarà, teorico. Ma ricordate: gli attacchi migliorano sempre, non peggiorano mai. Altri svilupperanno risultati migliori da questi numeri. Non c'è motivo di spaventarsi, non c'è ragione di smettere di usare AES, né di insistere che il NIST scelga un altro standard crittografico, ma questo sarà certamente un problema per alcune delle funzioni hash basate su AES candidate al concorso SHA-3.

<https://cryptolux.uni.lu/mediawiki/uploads/1/1a/Aes-192-256.pdf>  
[https://cryptolux.org/FAQ\\_on\\_the\\_attacks](https://cryptolux.org/FAQ_on_the_attacks)

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

MD6 ritirato dal concorso SHA-3

Sempre parlando di SHA-3, Ron Rivest ha suggerito che il suo algoritmo MD6 sia ritirato dal concorso SHA-3. Da un'email alla mailing list del NIST: "A nostro parere MD6 non è ancora pronto per il prossimo round di SHA-3; mettiamo inoltre a disposizione del NIST alcuni suggerimenti con l'avanzare del concorso".

"In sostanza, il problema di MD6 è che per essere sufficientemente veloce da poter essere competitivo, i progettisti devono ridurre il numero di round a 30-40, e a quei round l'algoritmo perde le sue prove di resistenza contro gli attacchi differenziali. Pertanto, se da un lato MD6 sembra un algoritmo crittografico hash robusto e sicuro, e presenta molte qualità per i processori multi-core, la nostra incapacità nel fornire una prova di sicurezza per una versione a round ridotti (e possibilmente modificata) di MD6 contro attacchi differenziali implica che MD6 non è pronto per essere preso in considerazione al prossimo round di SHA-3".

È un ritiro molto elegante, come ci si aspetterebbe da Ron Rivest, specialmente se si considera che non vi sono attacchi contro di esso, mentre altri algoritmi sono stati seriamente compromessi e i loro autori cercano continuamente di far finta che nessuno se ne sia accorto.

Rimandi:

<<http://groups.csail.mit.edu/cis/md6/>>

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

<[http://groups.csail.mit.edu/cis/md6/OFFICIAL\\_COMMENT\\_MD6\\_2009-07-01.txt](http://groups.csail.mit.edu/cis/md6/OFFICIAL_COMMENT_MD6_2009-07-01.txt)>

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

<<http://www.schneier.com/blog/archives/2009/07/md6.html>>

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

Risultati crittanalitici ancora migliori contro SHA-1

La famiglia SHA (che credo sarebbe meglio chiamare famiglia MD4) di funzioni hash crittografiche è stata sotto attacco per un lungo periodo. Nel 2005 abbiamo visto la prima crittanalisi di SHA-1 che era più veloce della forza bruta: collisioni in operazioni hash  $2^{69}$ , in seguito migliorate a  $2^{63}$ . Un buon risultato, ma nulla di sconvolgente. Ma ricordiamoci il grande truismo della crittanalisi: gli attacchi migliorano sempre, non peggiorano mai. La settimana scorsa ci siamo avvicinati a qualcosa di sconvolgente. Un nuovo attacco può, almeno in teoria, trovare collisioni in operazioni hash  $2^{52}$  -- decisamente entro i limiti delle possibilità di calcolo. Assumendo che la crittanalisi sia corretta, dovremmo aspettarci una collisione SHA-1 vera e propria entro l'anno.

Si noti che questo è un attacco di collisione, non è un attacco pre-image. Molti impieghi delle funzioni hash non vengono intaccati dagli attacchi di collisione. In caso contrario, passate subito a SHA-2.

Questo è il motivo per cui il NIST sta amministrando un concorso SHA-3 alla ricerca di un nuovo standard hash. E qualunque algoritmo verrà scelto, non assomiglierà a

nessun algoritmo della famiglia SHA (ecco perché credo che bisognerebbe chiamarlo Advanced Hash Standard, o AHS).

Rimandi:

<[http://www.schneier.com/blog/archives/2005/02/sha1\\_broken.html](http://www.schneier.com/blog/archives/2005/02/sha1_broken.html)>  
<[http://www.schneier.com/blog/archives/2005/02/cryptanalysis\\_o.html](http://www.schneier.com/blog/archives/2005/02/cryptanalysis_o.html)>  
<<http://www.schneier.com/essay-074.html>>  
<<http://eprint.iacr.org/2009/259.pdf>>  
<<http://www.schneier.com/essay-249.html>>

Una copia di questo articolo, con i rimandi integrati nel testo, è disponibile sul mio blog:  
<[http://www.schneier.com/blog/archives/2009/06/ever\\_better\\_cry.html](http://www.schneier.com/blog/archives/2009/06/ever_better_cry.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](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.