

CRYPTO-GRAM
15 febbraio 2007

Scritta da Bruce Schneier
Fondatore e CTO di BT Counterpane

Edizione italiana curata da Communication Valley SpA

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-0702.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:

Quando la messinscena di sicurezza funziona
Real ID: costi e benefici
Le ristampe di Crypto-Gram
Considerazioni sulla divulgazione totale
Inviare fotografie agli operatori dei servizi di emergenza
Il programma registered traveler "Clear"
News
Il DRM in Windows Vista
Le news di BT Counterpane
La psicologia della sicurezza
Un nuovo standard hash sicuro
Commenti dei lettori

** **

Quando la messinscena di sicurezza funziona

La scorsa settimana, quando sono andato all'ospedale a trovare una coppia di amici e il loro bimbo appena nato, ho notato un dettaglio di sicurezza piuttosto interessante. Per prevenire il rapimento di neonati, tutti i bimbi portavano alla caviglia un bracciale con un tag RFID. Le porte del reparto maternità sono dotate di sensori, e se un neonato le oltrepassa suona un allarme.

Il sequestro di neonati è raro, ma è sempre un rischio. Negli ultimi 22 anni negli Stati Uniti vi sono stati 233 rapimenti. Circa 4 milioni di bambini nascono ogni anno, il che significa che un neonato ha una possibilità su 375.000 di essere rapito. Confrontiamo questo dato con il tasso di mortalità annuo negli Stati Uniti (uno su 145) e appare subito chiaro dove si trovano i veri rischi.

E la possibilità di uno su 375.000 non è un rischio di oggi. I tassi di sequestro di neonati si sono abbassati negli ultimi anni, soprattutto

grazie ai programmi educativi negli ospedali.

Dunque perché gli ospedali si prendono il disturbo di applicare braccialetti RFID? Credo che lo facciano in primo luogo per rassicurare le madri. Durante il soggiorno in ospedale, i dottori hanno più volte portato via il figlio dei miei amici per effettuare vari esami. Milioni di anni di evoluzione hanno creato un legame fortissimo fra i genitori e il figlio appena nato: i braccialetti RFID sono una soluzione a basso costo per assicurare che i genitori stiano più tranquilli quando il bambino non si trova con loro.

La sicurezza è insieme una realtà e una percezione. La realtà della sicurezza è matematica, basata sulla probabilità di svariati rischi e l'efficacia di diverse contromisure. Conosciamo i tassi di sequestro di neonati e come i braccialetti RFID abbassino quei tassi. Conosciamo inoltre il costo di quei braccialetti, e possiamo quindi valutare se siano una misura di sicurezza efficace o meno. Ma la sicurezza è anche qualcosa che viene percepito, che si basa sulle reazioni psicologiche del singolo verso i rischi e le contromisure. E le due cose sono differenti: si può essere sicuri anche senza sentirsi sicuri, e ci si può sentire sicuri pur non essendo veramente sicuri.

I braccialetti RFID sono quel che ho preso a chiamare 'messinscena di sicurezza', ossia un tipo di sicurezza pensata specialmente per far sentire la gente più al sicuro. Ne ho sempre dette di tutti i colori sulle messinscene di sicurezza, considerandole uno spreco. Ma non è sempre e del tutto così.

È uno spreco se si considera esclusivamente la realtà della sicurezza. A volte le persone si sentono meno sicure di quanto in realtà sono. In questi casi (come per le mamme e la minaccia del sequestro di neonati), una contromisura palliativa creata primariamente per aumentare il senso di sicurezza è proprio quel che ci vuole.

Le confezioni resistenti alla manomissione per i medicinali senza ricetta hanno iniziato a comparire negli anni Ottanta, in risposta ad alcuni casi di avvelenamento molto pubblicizzati. Come contromisura, sono in gran parte una messinscena di sicurezza. È semplice avvelenare molti cibi e medicinali in libera vendita attraversando sigilli e involucri (con una siringa, per esempio), o aprire e sostituire il sigillo talmente bene che un ignaro cliente non se renderà nemmeno conto. Ma negli anni Ottanta esisteva un terrore diffuso per l'avvelenamento casuale di medicinali in libera vendita, e le confezioni resistenti alla manomissione hanno portato la percezione del rischio da parte del pubblico ad allinearsi con il livello di rischio reale: minimo.

Molta della sicurezza post-11 settembre può essere spiegata in quest'ottica. Ho spesso portato l'esempio delle truppe della Guardia Nazionale disposte negli aeroporti subito dopo gli attacchi terroristici e del fatto che le loro pistole fossero scariche. Come misura di sicurezza, la presenza dei militari non aveva senso. Non avevano l'addestramento necessario per migliorare la sicurezza ai checkpoint, né per essere un altro paio di occhi utili. Ma per trasmettere il messaggio "va tutto bene, si può volare" a un pubblico impaurito, è stata forse la cosa più giusta da fare.

Le messinscene di sicurezza, inoltre, affrontano il rischio accessorio delle cause legali. Esse vengono definitivamente decise dalle giurie, oppure si giunge a un accordo per evitare un processo legale, e le giurie basano le loro decisioni non solo sui fatti, ma anche sulle percezioni. Non è sufficiente, per un ospedale, presentare i dati statistici sul sequestro di neonati e dichiarare giustamente che non vale la pena implementare i braccialetti RFID; l'altra parte farà deporre una madre in lacrime e porterà la disputa sul lato emotivo. In

questi casi, la messinscena di sicurezza offre una sicurezza effettiva contro la minaccia di una causa legale.

Come la sicurezza reale, la messinscena di sicurezza ha un costo. Può costare denaro, tempo, concentrazione, libertà, e così via. Può costare in termini di riduzione delle cose che possiamo fare. Molte delle messinscene di sicurezza sono un pessimo compromesso poiché i costi superano i benefici in grande misura. Ma esistono casi in cui un pizzico di messinscena può avere senso.

Produciamo compromessi di sicurezza intelligenti (e intendo compromessi di sicurezza reale) quando la nostra percezione di sicurezza è praticamente allineata con la realtà delle cose. Quando i due elementi non sono allineati, non produciamo buona sicurezza o non la sappiamo applicare nella giusta maniera. La messinscena di sicurezza non è un sostituto della sicurezza vera e propria ma, se impiegata correttamente, può essere un sistema per aumentare la nostra percezione della sicurezza in modo che si avvicini di più alla realtà della sicurezza. Ci fa sentire più sicuri quando lasciamo che dottori e infermiere si prendano cura dei nostri bimbi, quando acquistiamo medicinali senza ricetta, quando voliamo. Insomma, ci aiuta a sentirci sicuri come se avessimo in mano i fatti e avessimo fatto i conti correttamente.

Naturalmente, se si esagera con le messinscene di sicurezza, la nostra percezione di sicurezza può superare la realtà delle cose, e questo non va bene. E altre persone (uomini politici, aziende, ecc.) possono sfruttare la messinscena di sicurezza per farci sentire più sicuri senza impegnarsi a lavorare duramente per renderci davvero più sicuri. Questo è il modo con cui viene solitamente utilizzata la messinscena di sicurezza ed è per questo che ne parlo spesso in termini negativi.

Ma scartarla completamente significa ignorare la percezione della sicurezza. E non funzionerà mai finché vi saranno persone coinvolte nei compromessi di sicurezza.

Questo articolo è originariamente apparso su Wired.com ed è dedicato al mio nuovo figlioccio, Nicholas Quillen Perry.

<http://www.wired.com/news/columns/0,72561-0.html>

Sequestri di neonati:

<http://www.saione.com/ispletter.htm>

Il post nel mio blog:

http://www.schneier.com/blog/archives/2007/01/in_praise_of_se.html

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

Real ID: costi e benefici

L'argomentazione era così ovvia che non aveva bisogno di essere ribadita. Alcuni hanno pensato che saremmo tutti più al sicuro (dal terrorismo, dal crimine, perfino dalla scomodità) se possedessimo un documento d'identità migliore. Un buon documento d'identità nazionale difficile da falsificare è un gioco da ragazzi (così almeno sostiene l'argomentazione), ed è ridicolo che un paese moderno come gli Stati Uniti non ne abbia uno.

Eppure moltissimi cittadini americani si sono sempre opposti a un documento d'identità nazionale, e continuano a esserlo. Solo immediatamente dopo l'11 settembre i sondaggi hanno mostrato una leggera maggioranza (51%) a favore, ma ben presto è tornata a essere un'opinione di minoranza. Di conseguenza entrambi i partiti politici si sono opposti alla carta d'identità, e quindi l'unico sistema per farla diventare

legge è stato introdurla tacitamente.

Ed è quel che ha fatto il deputato repubblicano F. James Sensenbrenner, del Wisconsin. Nel febbraio 2005 ha unito il Real ID Act a un progetto legge di stanziamento per la difesa. Nessuno avrebbe corso il rischio di non fornire supporto alle truppe fermando il progetto di legge, e così è entrato in vigore. Senza udienze, senza dibattito politico, in quasi totale silenzio, gli Stati Uniti si sono ritrovati con un documento d'identità nazionale.

Obbligando tutti gli stati a conformarsi a regole comuni e più severe per l'emissione delle patenti di guida, il Real ID Act trasforma le patenti in un documento d'identità nazionale de facto. È un obbligo enorme e non finanziato imposto agli stati e, naturalmente, questi hanno opposto resistenza. Il Dipartimento per la Sicurezza Nazionale sta ancora lavorando alle regole in dettaglio e alle tabelle di marcia, e si tratta dei particolari che determineranno esattamente quanto costoso e oneroso è questo programma.

È basandosi su questo sfondo che la National Governors Association, la National Conference of State Legislatures, e l'American Association of Motor Vehicle Administrators hanno cercato di stimare il costo di questa iniziativa. "The Real ID Act: National Impact Analysis" (Il Real ID Act: Analisi dell'impatto nazionale) è un rapporto meticoloso e dettagliato, e tutto quel che segue il sommario probabilmente annoierà qualunque tipo di lettore. Ma il rigore è importante, perché gli stati vogliono utilizzare questo documento per influenzare sia i dettagli tecnici, sia la tabella di marcia del Real ID. Le valutazioni sono conservative, e non lasciano spazio a problemi, ritardi o spese impreviste, ma si parla comunque di un costo totale di 11 miliardi di dollari per i primi cinque anni del programma.

Se non altro, è sorprendentemente a buon mercato: solo 37 dollari a persona per una stima di 295 milioni di individui che otterrebbero un nuovo ID sotto questo programma. Rimane comunque una cifra ingente. La domanda da porsi è, ovviamente: i benefici di sicurezza che avremmo in cambio valgono gli 11 miliardi di dollari? Abbiamo una stima dei costi; quel che manca adesso è una valutazione sulla sicurezza.

Proverò a farla io.

Quando la maggior parte delle persone pensa ai documenti di identità, si immagina una tessera plastificata con il nome e una foto. Non è sbagliato, ma è solamente una piccola parte di un qualsiasi sistema di documenti di identità. Quel che all'inizio sembra un dispositivo di sicurezza piuttosto semplice (una tessera che associa un nome a una foto), si tramuta ben presto in un sistema di sicurezza davvero complesso.

Non è tanto importante la bontà del Real ID quando viene utilizzato dalle centinaia di milioni di persone oneste che lo possiedono; ciò che importa è come il sistema possa fallire se utilizzato da qualcuno che ha intenzione di sovvertirlo. Come fallisce naturalmente, come può essere fatto fallire e come è possibile sfruttare le vulnerabilità di tale sistema.

Il primo problema è la tessera medesima. Non importa quanto la si rende difficile da falsificare, prima o poi verrà falsificata. Si può alzare il prezzo da pagare in caso di frode, ma non rendere il documento impossibile da falsificare. I Real ID verranno contraffatti.

Ancora peggio, ci sarà chi otterrà documenti d'identità legittimi ma sotto falso nome. Due dei terroristi dell'11 settembre possedevano patenti di guida valide dello stato della Virginia ma con nomi fittizi. E anche se potessimo garantire l'incorruttibilità di qualsiasi addetto

all'emissione di documenti d'identità nazionali, le tessere vengono emesse basandosi su altri documenti di identità, tutti molto più semplici da contraffare.

Né possiamo assumere che tutti saranno sempre in possesso di un Real ID. Attualmente ogni anno circa il 20% di tutti i documenti d'identità viene perduto. Occorrerebbe sviluppare un intero sistema di sicurezza differente solo per le persone che hanno smarrito la loro tessera d'identità, un sistema che potrebbe essere soggetto ad abusi.

In più, qualsiasi sistema di identificazione implica la presenza umana: e gli esseri umani commettono degli errori. Tutti abbiamo sentito storie di barman che si sono fatti ingannare da documenti falsi, o di controlli di sicurezza superficiali negli aeroporti e negli edifici governativi. Non è solo questione di addestramento: controllare i documenti di identità è un compito incredibilmente noioso e ripetitivo, ed è scontato che si commettano degli errori. Dati biometrici come le impronte del pollice potrebbero essere di aiuto, ma portano con sé tutta un'altra serie di vulnerabilità sfruttabili da un aggressore.

Tutti questi problemi dimostrano che i controlli di identità basati sul Real ID non saranno affatto sicuri come si spera. Ma il problema principale con qualsiasi tipo di sistema di identificazione forte è la necessità di un database. In questo caso specifico, dovrebbe essere composto da una rete di 50 altri database di informazioni private e sensibili su ogni cittadino americano, un database accessibile istantaneamente da ogni luogo: dai check-in degli aeroporti, dalle auto della polizia, dalle scuole, e così via.

I rischi di sicurezza di un tale database sono enormi. Non sarebbe altro che un ammasso di database già esistenti che sono incompatibili, pieni di dati errati, e in ultima analisi inaffidabili. Gli informatici non sanno come proteggere un database di queste dimensioni, né da hacker esterni, né dalle migliaia di impiegati autorizzati ad accedervi dall'interno.

Ma anche se potessimo risolvere tutti questi problemi, e se riuscissimo a rimanere nel budget di 11 miliardi di dollari, non otterremmo comunque una gran sicurezza. L'affidarsi a tessere di identità si basa su un mito della sicurezza decisamente pericoloso: se si conoscessero tutte le persone, si potrebbero estrapolare i malviventi dalla folla.

In un mondo ideale, quel che si vorrebbe è una specie di documento di identificazione che indicasse le intenzioni. Vorremmo che tutti i terroristi avessero una tessera con scritto sopra "malfattore", mentre tutte le altre persone avrebbero una tessera con la dicitura "persona onesta che non ha intenzione di dirottare aerei o di effettuare attentati dinamitardi". Allora la sicurezza sarebbe facile: basterebbe dare un'occhiata ai documenti d'identità della gente e, nel caso ci si imbattesse in qualche malfattore, gli si impedirebbe l'accesso a bordo dell'aereo o all'interno di un edificio.

Tutto ciò è ovviamente ridicolo; pertanto ci affidiamo all'identità. In teoria, se sapessimo chi siete, e se avessimo sufficienti informazioni sul vostro conto, potremmo prevedere in qualche modo le vostre intenzioni più o meno malevole. Ma questo è altrettanto ridicolo.

Ancora peggio, non appena si dividono le persone in due categorie, individui maggiormente degni di fiducia e individui meno fidati, si crea automaticamente una terza categoria molto pericolosa: persone indegne di fiducia dei quali però non si ha ragione di diffidare. Il bombarolo di Oklahoma City, Timothy McVeigh; i cecchini di Washington DC; i dinamitardi della metropolitana di Londra; e molti dei terroristi dell'11 settembre non avevano alcun legame precedente con il terrorismo. I malfattori possono rubare l'identità e il profilo di una persona

onesta. Il profiling può avere come risultato una sicurezza minore se si offre ad alcune categorie di persone un sistema facile per oltrepassare i controlli di sicurezza.

Ed esiste un'altra modalità di errore, ancora più pericolosa, per questi sistemi: persone oneste che rispondono perfettamente al profilo del malfattore. Dato che i malfattori sono molto rari, quasi chiunque risponda al profilo del criminale si rivelerà essere un falso allarme. Pensate a tutti i problemi connessi alla no-fly list del governo. Quella lista, con la quale verranno confrontati i Real ID, non solo spreca risorse investigative che sarebbero meglio impiegate in altre attività, ma provoca anche gravi conseguenze agli innocenti che corrispondono al profilo.

Basta parlare di terrorismo, ora. Prendiamo in esame problematiche più banali, come il furto di identità. Perversamente, una tessera d'identità difficile da contraffare può in realtà far aumentare il rischio di furto di identità. Un'unica onnipotente tessera di identità sarà considerata fidata in sempre più occasioni e utilizzata in molti più contesti. Perciò un individuo che riesca effettivamente a contraffarla (o a ottenerne una sotto falso nome) potrà commettere un maggior numero di frodi. Un sistema di documenti d'identità centralizzato è un rischio di sicurezza molto più grave di un sistema decentralizzato con varie organizzazioni che emettono tessere d'identità secondo regole e finalità proprie.

La sicurezza è sempre un compromesso, e costi e benefici devono equilibrarsi. È un procedimento che facciamo intuitivamente. Pochi di noi se ne vanno in giro indossando giubbotti antiproiettile. Non è perché non sono efficaci, ma perché la maggioranza delle persone ritiene che non valga la pena accettare il compromesso. Non vale il denaro, la seccatura, la perdita di uno stile nel vestire. Se vivessimo in un paese devastato dalla guerra come l'Iraq, probabilmente faremmo dei compromessi totalmente diversi.

Il Real ID è un altro di quei pessimi compromessi di sicurezza. Costerà agli Stati Uniti almeno 11 miliardi di dollari, e non otterremo molta protezione in cambio. Il rapporto suggerisce una serie di misure ideate per sgravare gli stati dagli oneri finanziari: posticipare le scadenze per la conformità, permettere sistemi di verifica manuale, e così via. Ma quel che non suggerisce è la soluzione più semplice e più efficace: eliminare del tutto il programma Real ID. Per il prezzo che tocca pagare, non ci avvicineremo neanche alla sicurezza che meriteremmo.

Questo articolo apparirà nel numero di marzo/aprile del "Bulletin of Atomic Scientists".

REAL-ID:

<http://thomas.loc.gov/cgi-bin/bdquerytr/z?d109:HR01268:>

"The REAL-ID Act: National Impact Analysis" [Il Real ID Act: Analisi dell'impatto nazionale]:

<http://www.nga.org/Files/pdf/0609REALID.pdf>

Ci sono delle novità sull'argomento. Il Maine è il primo stato a rigettare REAL-ID. Questo significa che una patente di guida rilasciata dallo stato del Maine non verrà considerata valida a livello federale, anche se sono certo che i Federali torneranno sulle loro decisioni a riguardo. A mio avviso il Montana sarà il secondo stato a rifiutare REAL-ID e il New Mexico sarà il terzo.

<http://www.northcountrygazette.org/articles/2007/012807RealID.html>

http://www.usatoday.com/news/nation/2007-01-30-realID_x.htm

Maggiori informazioni su REAL-ID:

<http://www.realigntmare.org>

Si è dovuto attendere che i ricercatori pubblicassero una documentazione esaustiva delle vulnerabilità perché le aziende di software iniziassero a sistemarle.

Com'è ovvio, i produttori di software odiavano tutto questo. La loro immagine veniva messa in cattiva luce ogni volta che una vulnerabilità era divulgata, e l'unico sistema per ottenere della buona pubblicità era quello di rilasciare rapidamente una patch. Per un colosso come Microsoft si trattava di un'operazione costosissima.

Perciò un gruppo di aziende di software e alcuni ricercatori di sicurezza si sono associati e hanno inventato la "responsible disclosure", la divulgazione responsabile. L'idea di fondo è che la minaccia di pubblicare una vulnerabilità è quasi efficace quanto pubblicarla davvero. Un ricercatore responsabile quindi, prima di divulgare pubblicamente una certa vulnerabilità, dava tacitamente un po' di vantaggio all'azienda di software per produrre la patch necessaria.

È stata una buona idea (ed è la prassi odierna), ma che è stata possibile soltanto perché la divulgazione totale era la norma. Ed è sempre una buona idea purché la minaccia rimanga la divulgazione totale.

Qui la morale non si applica soltanto al software, è più generale. L'esame pubblico è essenziale per il progressivo miglioramento della sicurezza, che si parli di software, di sicurezza negli aeroporti o di misure antiterrorismo governative. Certo, esistono dei compromessi. Divulgazione totale significa che anche i malintenzionati vengono a conoscenza della vulnerabilità insieme al resto di noi (a meno che, ovviamente, non lo siano venuti a sapere prima), ma nella maggior parte dei casi i benefici superano di gran lunga gli svantaggi.

La segretezza impedisce alle persone di valutare con esattezza i propri rischi. La segretezza impedisce il dibattito pubblico sulla sicurezza e inibisce l'educazione alla sicurezza che porta a fare progressi. La segretezza non migliora la sicurezza: la soffoca.

Preferisco avere tutte le informazioni possibili per prendere una decisione informata sulla sicurezza, che si tratti di acquistare un prodotto software o di decidere quale fra due partiti politici votare. Preferisco avere le informazioni che ho bisogno per esercitare pressioni sui produttori di software affinché migliorino la sicurezza.

Non voglio vivere in un mondo in cui le aziende possano vendermi del software che sanno essere pieno di buchi o in cui il governo possa mettere in atto misure di sicurezza senza assumersi la responsabilità. Preferisco di gran lunga un mondo in cui ho tutte le informazioni che necessito per valutare e proteggere la mia sicurezza.

Questo articolo è originariamente apparso su CSOnline:

<http://www2.csoonline.com/exclusives/column.html?CID=28073>

Fa parte di una serie di scritti sull'argomento. Marcus Ranum ha scritto contro la pratica di divulgare vulnerabilità:

<http://www2.csoonline.com/exclusives/column.html?CID=28072>

Mark Miller di Microsoft ha scritto a favore della divulgazione responsabile.

<http://www2.csoonline.com/exclusives/column.html?CID=28071>

Sono tutti interventi supplementari a un articolo veramente interessante del "CSO Magazine", dal titolo "The Chilling Effect" sulla confluenza di forze che stanno rendendo più difficile la ricerca e la divulgazione di vulnerabilità nel software basato sul Web:

http://www.csoonline.com/read/010107/fea_vuln.html

Tutti i link meritano una lettura integrale.

Il programma registered traveler "Clear"

CLEAR, un servizio privato che effettua il pre-screening dei passeggeri per una quota annua di 100 dollari, è arrivato al Kennedy International Airport. Per beneficiare del programma registered traveler Clear, che è gestito da Verified Identity Pass, il passeggero deve compilare un modulo, lasciare le proprie impronte digitali e una scansione della retina, e presentare due forme di identificazione. Se il viaggiatore supera un background check federale, riceverà una tessera che gli permetterà di oltrepassare velocemente la sicurezza aeroportuale.

Sembra una bella cosa, ma si tratta in realtà di due idee riunite in una: un'idea è intelligente, l'altra è molto stupida.

L'idea intelligente è lasciare che la gente paghi per un servizio migliore. Clear è in attività all'Orlando International Airport sin da luglio 2005 e i suoi iscritti hanno potuto superare i checkpoint di sicurezza più in fretta semplicemente perché vengono separati da passeggeri meno esperti che non conoscono le procedure.

Ora, al Kennedy e in altri aeroporti, Clear sta acquistando e installando tecnologia approvata a livello federale che velocizzerà ulteriormente il processo di screening: scanner che sollevano i tesserati dall'obbligo di togliersi le scarpe, e macchine per il rilevamento di esplosivi che elimineranno l'obbligo di togliersi giacche e cappotti. Vi sono anche degli impiegati Clear ai checkpoint. Non possono effettuare lo screening dei tesserati, ma servono per assistere i tesserati durante le fasi di controllo di sicurezza. Clear non ha ancora pagato gli aeroporti per avere una corsia di sicurezza in più, né la Transportation Security Administration per avere personale extra per lo screening dei passeggeri, ma entrambe queste possibilità sono previste in caso si superi una certa quota di adesioni.

Io faccio più di 200.000 miglia in aereo ogni anno e sarei disposto ben volentieri a pagare 100 dollari annui per superare i controlli di sicurezza aeroportuali con maggior celerità.

Ma l'idea stupida è il background check. Quando furono inizialmente concepiti, i programmi 'traveler' si concentravano sul pre-screening. Viaggiatori precedentemente verificati superavano i checkpoint di sicurezza sottoposti a minor controllo, e le risorse sarebbero state impiegate per effettuare lo screening delle altre persone. Sembra ragionevole, ma ci renderebbe tutti meno sicuri.

I background check si basano sul pericoloso mito di sicurezza per cui sia in qualche modo possibile estrapolare i terroristi da una grande quantità di persone se potessimo identificare chiunque. Purtroppo non esiste alcun profilo terroristico che un pre-screening possa rivelare. Timothy McVeigh sarebbe probabilmente riuscito a ottenere una di queste tessere. Così come Eric Rudolph, il bombarolo delle Olimpiadi del 1996 ad Atlanta. Non esiste nemmeno un elenco attendibile di terroristi conosciuti con cui effettuare dei raffronti; la lista governativa usata dalle linee aeree è stato il bersaglio preferito di beffe e critiche per anni.

E ci siamo forse dimenticati dell'attuale prevalenza del furto di identità? Se pensate che un criminale che si sostituisce a voi nel rapporto con la vostra banca sia un problema, aspettate quando inizierà a farlo con la Transportation Security Administration.

Il fatto è che ogni volta che si creano due percorsi per passare attraverso i checkpoint, uno ad alta sicurezza, l'altro a bassa sicurezza, occorre prevedere che i malviventi troveranno un sistema per

Il Washington Post sulla sorveglianza onnipresente:

<http://www.washingtonpost.com/wp-dyn/content/article/2007/01/15/AR2007011501304.html>

oppure <http://tinyurl.com/y86fyl>

Dopo oltre cinque anni di vessazioni ai danni di innocenti e la cattura di nessun terrorista, la no-fly list verrà finalmente esaminata per controllarne l'accuratezza, e probabilmente dimezzata.

<http://www.breitbart.com/news/2007/01/17/D8MNE7DGO.html>

Non basta, però. La no-fly list non funziona ed è semplice da aggirare.

<http://www.schneier.com/essay-052.html>

http://www.schneier.com/blog/archives/2006/11/forge_your_own.html

<http://www.cs.berkeley.edu/~daw/faa/noid.html>

<http://www.schneier.com/essay-008.html>

http://www.schneier.com/blog/archives/2006/10/nofly_list.html

Tatuaggi RFID. Ottima idea per il bestiame. Pessima idea se impiegata sui soldati:

<http://www.industrialcontroldesignline.com/showArticle.jhtml?articleID=196900052>

oppure <http://tinyurl.com/2mk9g3>

Grande furto online ai danni di una banca svedese. Questa è la parte che preferisco: "Ehlin ha dichiarato che la colpa di tutto è stata un attacco di social engineering andato a buon fine, e che non vi è stata nessuna lacuna nelle procedure di sicurezza di Nordea". Ma questo tipo è un idiota o cosa?

<http://news.zdnet.co.uk/security/0,1000000189,39285547,00.htm>

Al secondo posto nella serie di stupide dichiarazioni alla stampa, ecco il commento dell'assistant city manager di Kansas City a seguito della perdita di 26 nastri contenenti dati sensibili: "Non è una situazione per cui sarebbe possibile avere accesso alle informazioni con un portatile... Per leggere quei nastri è necessaria dell'attrezzatura speciale e delle conoscenze specifiche".

<http://www.myfoxkc.com/myfox/pages/News/Detail?contentId=2113498&version=4&locale=EN-US&layoutCode=TSTY&pageId=3.1.1>

oppure <http://tinyurl.com/2a35bh>

La NSA offre una opportunità di lavoro come data miner:

http://www.issa-balt.org/html/ctc_opportunity.html

Truppe SAS di stanza a Londra:

<http://www.timesonline.co.uk/article/0,,2-2559186,00.html>

Se da una parte concordo sul fatto che la polizia britannica ha fatto un gran pasticcio con il caso Menezes, non sono però del tutto convinto che il SAS possa fare di meglio. Le forze di polizia vengono addestrate per muoversi all'interno di una società regolata da leggi; le unità militari vengono addestrate principalmente per operazioni militari di combattimento. Quale fra i due gruppi pensate che sarà più calmo e controllato? Questo genere di cose è uno dei risultati della retorica della "guerra al terrore". Non abbiamo bisogno di operazioni militari, ma di protezione di polizia. Secondo me certa gente ha visto troppe stagioni di "24".

Sir Ken McDonald, il "direttore dei processi pubblici" è intervenuto contro la retorica della "guerra al terrore":

<http://politics.guardian.co.uk/terrorism/story/0,,1997247,00.html>

Il sistema DRM di Blu-Ray è stato violato, anche se i dettagli sono scarsi. È la stessa persona che ha compromesso il sistema HD DVD a dicembre (entrambi fanno uso di AACs). Come ho scritto in precedenza, questi due sistemi dovrebbero essere entrambi progettati per ripristinarsi a seguito di simili attacchi. Staremo a vedere se la

feature di ripristino funzionerà.

http://www.theregister.co.uk/2007/01/23/blu-ray_drm_cracked/

Consiglio la lettura di questa serie in sette parti scritta da Ed Felten sull'argomento:

<http://www.freedom-to-tinker.com/?p=1104>

<http://www.freedom-to-tinker.com/?p=1106>

<http://www.freedom-to-tinker.com/?p=1107>

<http://www.freedom-to-tinker.com/?p=1108>

<http://www.freedom-to-tinker.com/?p=1109>

<http://www.freedom-to-tinker.com/?p=1110>

<http://www.freedom-to-tinker.com/?p=1111>

"Prophetic Justice" [Giustizia profetica] di Amy Waldman ("The Atlantic Monthly", ott. 2006) è un articolo affascinante sui processi di terrorismo negli Stati Uniti in cui l'accusa cerca di provare che l'imputato stava pensando di commettere un atto terroristico. Assai di frequente, i processi sono incentrati su varie interpretazioni dell'Islam, delle scritture islamiche e del credo islamico, e spesso è la religione che viene messa sotto accusa. Leggendolo, mi ha molto colpito una certa retorica religiosa fra le più estremiste che vi siano oggi negli Stati Uniti, e sarei curioso di vedere come la spunterebbe se sottoposta allo stesso livello di scrutinio. È un articolo lungo, ma vale assolutamente la pena leggerlo. Vi sono innumerevoli problemi quando si persegue qualcuno per reati di pensiero, e l'articolo ne mette in luce alcuni.

<http://www.theatlantic.com/doc/200610/waldman-islam>

Ho già scritto di come le uniformi ufficiali siano mezzi di autenticazione intrinseca, anche se è facile contraffarle. Ora questa tattica viene sfruttata dagli insorgenti a Baghdad:

<http://www.washingtonpost.com/wp-dyn/content/article/2007/01/21/AR2007012100227.html>

oppure <http://tinyurl.com/yv6hcd>

http://www.schneier.com/blog/archives/2007/01/iraqi_gunmen_dr.html

Un gioco di sicurezza aeroportuale: giocate online e provate a stare al passo con le regole arbitrarie che cambiano in continuazione.

<http://www.addictinggames.com/airportsecurity.html>

"Internet Explorer insicuro per 284 giorni nel 2006".

http://blog.washingtonpost.com/securityfix/2007/01/internet_explorer_unsafe_for_2.html

oppure <http://tinyurl.com/y4qnyt>

<http://www.washingtonpost.com/wp-srv/technology/daily/graphics/index20070104.html>

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

Una proposta in Scozia per proteggere le telecamere degli autovelox dai vandali controllandole con altre telecamere. Suppongo che poi saranno necessarie altre telecamere per proteggere le telecamere che controllano le telecamere. Avrò mai fine tutto ciò?

http://news.bbc.co.uk/2/hi/uk_news/scotland/south_of_scotland/6293823.stm

oppure <http://tinyurl.com/2ql8rs>

La vicenda affascinante di un automobilista israeliano che ha dato un passaggio a un bombarolo suicida. Ciò che mi sembra interessante è come l'automobilista giunge a rendersi conto che il passeggero è un bombarolo suicida. Niente che possa emergere in un "profilo", ma la sensazione che qualcosa non va.

http://news.bbc.co.uk/1/hi/world/middle_east/6312657.stm

L'eccesso di segretezza e sicurezza non fa altro che aiutare i terroristi. L'ho detto più di una volta, e adesso lo dice anche il direttore dei servizi di intelligence canadesi:

<http://www.canada.com/ottawacitizen/news/story.html?id=5f848011-0a8c-4348-90df-f6656d0281d9>
oppure <http://tinyurl.com/2koeb9>

"Knowing the Enemy" [Conoscere il nemico] di George Packer ("The New Yorker", 18 dicembre 2006) è un articolo molto interessante sulla scienza sociale necessaria per prevalere contro il terrorismo islamico che, l'autore sostiene, sarebbe meglio definire come contro-insorgenza.
http://www.newyorker.com/fact/content/articles/061218fa_fact2

Modelli di business, legali e illegali, per scoprire vulnerabilità di sicurezza. Si sparge molto FUD in questo articolo, ma vi sono anche buoni spunti.
<http://www.iht.com/articles/2007/01/29/business/bugs.php>

Dave Barry sulla sicurezza del Super Bowl:
http://www.miami.com/mld/miamiherald/living/columnists/dave_barry/16601599.htm?source=rss&channel=miamiherald_dave_barry
oppure <http://tinyurl.com/yoxd73>

Secondo un vecchio articolo, "L'errata identificazione operata da testimoni oculari è la causa principale che porta alla detenzione di innocenti". Visto quel che ho letto recentemente sulla memoria e sul cervello, non mi sorprende affatto. Lo stato del New Mexico sta ora discutendo una legge che riformi le procedure di identificazione da parte di testimoni oculari. Non ho accesso a nessuno degli studi di psicologia e criminologia su cui si poggiano tali riforme, ma la legge viene sostenuta da persone in gamba.
http://www.lcsun-news.com/ci_5164992

Un affascinante articolo sul bunker di Corsham, il sito sotterraneo segreto del Regno Unito in cui si sarebbe ritirato il governo in caso di guerra nucleare.
<http://politics.guardian.co.uk/politicspast/story/0,,2006099,00.html>

Una serie di dati interessanti da New York. Il numero delle persone fermate e perquisite è quintuplicato dal 2002, ma il numero di arresti a seguito di questi fermi è solo raddoppiato. (Anche il numero di mandati di comparizione è quintuplicato).
<http://www.prisonplanet.com/articles/february2007/030207Stopped.htm>

Tre tubi bomba sono stati trovati nella cittadina di Pearblossom, California e, pare, eliminati senza causare isterismi. Voi di Boston, avete capito?
http://www.dailynews.com/ci_5180780

Ross Anderson e Tyler Moore hanno appena pubblicato "The Economics of Information Security: A Survey and Open Questions" [L'economia dell'information security: un'indagine e le questioni aperte]. Ottima lettura.
<http://www.cl.cam.ac.uk/~rja14/Papers/toulouse-summary.pdf>
http://www.cl.cam.ac.uk/~rja14/Presentations/econsec_toulouse.ppt
<http://www.cl.cam.ac.uk/~twm29/science-econ.pdf>

Questo articolo è l'illustrazione perfetta del tipo di spreco di risorse e stanziamenti ottenuti con manovre politiche che ci piace chiamare "sicurezza nazionale". E pensare che potremmo spendere questi soldi in qualcosa di veramente utile.
http://www.boston.com/news/local/articles/2007/02/09/firefighters_windfall_comes_with_a_catch/
oppure <http://tinyurl.com/yw4lew>

"Information Security and Externalities" [L'information security e le esternalità]. Ho aggiornato un mio articolo del 2004 per la newsletter trimestrale della European Network and Information Security Agency.

http://www.enisa.europa.eu/doc/pdf/publications/enisa_quarterly_01_07.pdf

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

Questo è un buon riassunto del caso europeo SWIFT legato alla privacy:
<http://www.newswireless.net/index.cfm/article/3057>

Tutti abbiamo visto quegli ologrammi anti-contraffazione: sulle carte di credito, sul software, su abiti costosi. Pare che stiano diventando più facili da contraffare.

<http://www.wired.com/news/technology/0,72664-0.html>

BitFrost, il sistema di sicurezza del progetto "Un portatile per ogni bambino", è molto interessante. Si leggano almeno i principi e gli obiettivi del disegno del sistema.

<http://wiki.laptop.org/go/Bitfrost>

www.wired.com/news/technology/0,72669-0.html

<http://it.slashdot.org/article.pl?sid=07/02/07/2137233>

Questo articolo parla di una tecnica di scansione cerebrale che legge le intenzioni delle persone. Non vi sono molti dettagli, ma a mio avviso non funziona molto bene. Ma non è questo il punto. Se non funziona oggi, funzionerà fra cinque, dieci, vent'anni; insomma, un giorno funzionerà. Quel che dobbiamo fare oggi è discutere gli aspetti legali ed etici di questo genere di interrogazioni.

<http://www.guardian.co.uk/science/story/0,,2009217,00.html>

Ho scritto di questo tipo di cose nel 2005, nel contesto delle udienze di conferma del giudice Roberts.

<http://www.wired.com/news/politics/0,1283,68911,00.html>

Una vignetta sui numeri casuali:

<http://xkcd.com/c221.html>

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

Il DRM in Windows Vista

Windows Vista comprende una serie di "funzionalità" assolutamente indesiderate. Tali funzionalità renderanno i computer meno affidabili e meno sicuri. Li renderanno meno stabili più lenti. Causeranno problemi di supporto tecnico. E in alcuni casi potrà essere necessario aggiornare le periferiche e il software che già possediamo. E queste funzionalità non fanno nulla di utile, anzi lavorano contro di noi. Si tratta di funzioni di gestione dei diritti digitali (DRM) incorporate in Vista per ordine dell'industria dell'intrattenimento.

E non si possono rifiutare.

I dettagli sono piuttosto tecnici, ma fondamentalmente Microsoft ha revisionato gran parte del nucleo del sistema operativo per aggiungere una tecnologia di protezione per nuovi formati media come i dischi ottici HD DVD e Blu-ray. Certi percorsi di output ad alta qualità, sia audio che video, sono riservati a periferiche protette. A volte la qualità di output viene degradata artificialmente; altre volte la riproduzione è del tutto inibita. E Vista impiega continuamente le risorse della CPU per monitorare se stesso, cercando di capire se l'utente sta cercando di fare qualcosa che Vista ritiene inopportuno. In caso questo avvenga, il sistema operativo limita le funzionalità e in casi estremi riavvia il sottosistema video. Non sappiamo ancora i dettagli precisi a riguardo e quando in profondità il sistema si spinga, ma le prospettive non sono buone.

Microsoft ha inserito in Vista tutte quelle feature che inibiscono le

funzionalità perché vuole dominare l'industria dell'intrattenimento. Questa ovviamente non è la versione dei fatti secondo Microsoft, che dichiara che non ha avuto scelta, che è Hollywood a esigere il DRM in Windows così da permettere la visione di "contenuti premium" (cioè quei film da poco usciti e che stanno ancora facendo profitti) sui nostri computer. Se Microsoft non si adeguasse, sarebbe relegata a un ruolo secondario perché Hollywood toglierebbe il supporto alla piattaforma Windows.

Sono tutte sciocchezze. Microsoft avrebbe potuto facilmente dire all'industria dell'intrattenimento che non avrebbe volontariamente castrato il proprio sistema operativo, punto e basta. Microsoft detiene il 95% del mercato dei sistemi operativi: quali alternative avrebbe avuto Hollywood? Certo, Big Media ha sempre sostenuto il DRM, ma di recente altri, come Sony dopo il disastro del 2005, ed EMI Group, stanno rivedendo le loro posizioni.

Quel che le aziende dell'intrattenimento stanno finalmente capendo è che il DRM non funziona, ed è solo un fastidio per i loro clienti. Come qualsiasi altro sistema DRM inventato finora, quello di Microsoft non impedirà ai pirati professionisti di copiare tutto ciò che vogliono. La sicurezza del DRM in Vista è stata compromessa il giorno stesso del rilascio di Vista. Certo, Microsoft ci metterà una patch, ma poi il sistema verrà compromesso nuovamente. Il solito braccio di ferro dove chi si difende non l'avrà mai vinta.

Credo che Microsoft lo sappia, e che sappia che non ha importanza. La questione non è fermare i pirati e quella piccola percentuale di persone che scaricano liberamente film da Internet. E non è nemmeno un discorso di preferenza di Microsoft verso Hollywood a scapito di chi fra noi paga per poter utilizzare Vista. Si tratta invece della stragrande maggioranza di utenti onesti da una parte e di chi possiede i canali per distribuire loro i contenuti dall'altra. E anche se è iniziata come una partnership, alla fine Microsoft finirà con l'obbligare le aziende cinematografiche a vendere contenuti nei suoi formati proprietari.

Abbiamo già visto questa tattica in azione: è ciò che ha fatto Apple con l'industria discografica. Inizialmente iTunes funzionava in accordo con le major discografiche per distribuire contenuti, ma ben presto Edgar Bronfman Jr., CEO di Warner Music, si è reso conto che non poteva dettare un modello di prezzi a Steve Jobs. La stessa cosa accadrà qui: quando Vista si sarà fortificato all'interno del mercato, Howard Stringer di Sony non sarà in grado di dettare prezzi o condizioni a Bill Gates. Questa è una guerra per la distribuzione cinematografica del XXI secolo, e quando la polvere tornerà a depositarsi, Hollywood non saprà che cosa l'ha colpita.

A essere onesti, giusto l'altra settimana Steve Jobs si è schierato pubblicamente contro il DRM in ambito musicale. È una posizione ragionevole, dal punto di vista del business, ora che Apple controlla il mercato della distribuzione musicale online. Ma Jobs non ha parlato di film, ed egli è il maggiore azionista Disney. Si fa presto a parlare. La vera domanda da porsi è: Jobs permetterà la riproduzione del contenuto comprato sull'iTunes Store anche su dispositivi Microsoft o Sony, oppure questa è soltanto un'abile strategia per deviare le accuse verso le già odiate etichette discografiche?

Microsoft sta cercando di ottenere molto di più: non solo Hollywood, ma anche i produttori di periferiche. Il DRM di Vista obbligherà gli sviluppatori di driver a conformarsi a ogni genere di regolamentazioni e a certificarsi, altrimenti i driver non funzioneranno. E Microsoft sta pensando di estendere questa situazione anche ai produttori indipendenti di software. È un'altra guerra per il controllo del mercato informatico.

Purtroppo noi utenti ci troviamo nel bel mezzo del fuoco incrociato. Non

suonare arcana e molto tecnica, ma le funzioni hash sono ciò che fa funzionare la moderna crittografia. Offrono sicurezza Web nell'SSL. Contribuiscono alla gestione delle chiavi nella crittografia email e vocale: PGP, Skype e tutto il resto. Rendono più difficile la scoperta delle password. Vengono utilizzate nei virtual private network, contribuiscono a fornire sicurezza DNS e assicurano che gli aggiornamenti software automatici siano legittimi. Mettono a disposizione ogni genere di funzioni di sicurezza nel sistema operativo. Ogni qual volta fate qualcosa su Internet che ha a che vedere con la sicurezza, da qualche parte ci sarà una funzione hash.

Sostanzialmente, una funzione hash è una funzione fingerprint. Riceve un input a lunghezza variabile (dal singolo byte a file lunghi terabytes) e lo converte in una stringa a lunghezza fissa: 20 byte, per esempio.

Le funzioni hash unidirezionali devono avere due proprietà. La prima: sono unidirezionali, a senso unico. Significa che è semplice prendere un input e calcolare il valore hash, ma è impossibile prendere un valore hash e ricreare la stringa originale. Con "impossibile" intendo dire "che non può essere effettuato in un intervallo di tempo ragionevole".

La seconda proprietà è l'essere prive di collisioni. Significa che, pur essendovi un numero infinito di input per ogni valore hash, non se ne troveranno mai due per un valore di hash. Anche in questo caso, quel "mai" è da intendersi come "l'impossibile" visto prima. Il ragionamento crittografico che sta alla base di queste due proprietà è un po' astruso, ma qualsiasi testo di crittografia parla delle funzioni hash.

La funzione hash che si utilizza più frequentemente è SHA-1. Inventata dalla National Security Agency, è in circolazione dal 1995. Di recente, tuttavia, hanno avuto luogo alcuni attacchi crittanalitici davvero impressionanti contro l'algoritmo. Il migliore di questi attacchi è a malapena fattibile, e non è efficace contro tutte le applicazioni di SHA-1. Ma c'è un vecchio detto all'interno della NSA: "Gli attacchi migliorano sempre, non peggiorano mai". È arrivato il momento di abbandonare SHA-1.

Vi sono delle alternative nel breve termine, un algoritmo collegato chiamato SHA-256 sembra la più ovvia, ma sono tutti basati su una famiglia di funzioni hash sviluppata inizialmente nel 1992. Negli ultimi 15 anni abbiamo imparato molte cose sull'argomento, e si può fare decisamente di meglio.

Perché il National Institute of Standards and Technology, però? Perché possiede esattamente l'esperienza e la reputazione che vogliamo. Ci siamo trovati nella stessa posizione con le funzioni crittografiche nel 1997. Occorreva trovare un sostituto del Data Encryption Standard, ma non era affatto ovvio quale dei candidati avrebbe dovuto essere. Il NIST decise di organizzare una competizione mondiale per un nuovo algoritmo crittografico. Vi furono 15 contributi da 10 paesi diversi (io facevo parte del gruppo che propose Twofish) e dopo quattro anni di analisi e crittanalisi, il NIST scelse l'algoritmo Rijndael affinché diventasse l'Advanced Encryption Standard, o AES.

La competizione AES è stata una delle cose più divertenti a cui ho partecipato in ambito crittografico. La si immagini come un grande incontro di demolizione crittografica: una manciata di noi esperti butta il proprio lavoro migliore sul ring e poi ce le diamo di santa ragione finché ne rimane in piedi solo uno. Beh, il tutto si è svolto in modi più accademici e strutturati, ma il processo ha stimolato molta ricerca nell'ideazione e nella crittanalisi dei block-cipher. Ho imparato tantissimo in materia, grazie alla competizione AES, e noi come comunità ne abbiamo beneficiato immensamente.

Il NIST ha fatto un ottimo lavoro nel gestire il processo che ha

condotto ad AES, pertanto è la scelta migliore fare altrettanto con le funzioni hash. Ed è ciò che sta facendo. L'anno scorso e l'anno precedente, il NIST ha sponsorizzato due workshop per discutere i requisiti di una nuova funzione hash, e lo scorso mese ha annunciato una competizione per selezionare un sostituto di SHA-1. I contributi devono essere mandati entro l'autunno del 2008 e la scelta di un unico standard è pianificata entro la fine del 2011.

Sì, è un programma ragionevole. Progettare una funzione hash sicura sembra più difficile che ideare un algoritmo crittografico sicuro, anche se non sappiamo se è dovuto alla matematica intrinseca, o semplicemente è il risultato delle nostre conoscenze imperfette. Per produrre un nuovo standard hash sicuro occorre tempo. Fortunatamente SHA-256 è una buona soluzione da utilizzare nel frattempo.

Adesso vogliate scusarmi, ma il team Twofish si deve ricostituire e iniziare a lavorare su una proposta di Advanced Hash Standard.

http://en.wikipedia.org/wiki/One-way_hash_function
<<http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenote.pdf>>
oppure <<http://tinyurl.com/yrxah>>

Crittanalisi di SHA-1:

<http://www.schneier.com/blog/archives/2005/02/cryptanalysis_o.html>
<http://www.schneier.com/blog/archives/2005/08/new_cryptanalyt.html>

AES:

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

Twofish:

<<http://www.schneier.com/twofish.html>>

La competizione Hash indetta dal NIST:

<<http://www.csrc.nist.gov/pki/HashWorkshop/index.html>>
<<http://www.csrc.nist.gov/pki/HashWorkshop//FederalRegister/Federal%20Register%20Notice%20for%20Requirements%20&%20Criteria%20-%20E7-927.pdf>>
oppure <<http://tinyurl.com/25mtrj>>
<<http://csrc.nist.gov/pki/HashWorkshop/timeline.html>>
<<http://www.csrc.nist.gov/pki/HashWorkshop/2005/program.htm>>
<http://www.csrc.nist.gov/pki/HashWorkshop/2006/program_2006.htm>

Questo articolo è originariamente apparso su Wired.com.

<<http://www.wired.com/news/columns/0,72657-0.html>>

Ogni volta che tratto le funzioni hash unidirezionali, ricevo delle risposte da parte di persone che sostengono che tali funzioni non possono essere sicure perché un numero infinito di testi viene ridotto al medesimo valore hash corto (160 bit, nel caso di SHA-1). Certo, ovviamente un numero infinito di testi si riduce al medesimo valore hash: è così che procede la funzione. Ma le probabilità che ciò accada naturalmente sono inferiori alla probabilità che le molecole d'aria si raggruppino tutte in un angolo della stanza, soffocandoci. E non è possibile nemmeno farlo accadere. Al momento, svariati gruppi di ricercatori stanno tentando di implementare l'attacco di Xiaoyun Wang contro SHA-1. Faccio questa predizione: quest'anno uno di loro troverà due testi che si riducono al medesimo valore hash; questo dimostrerà che la funzione hash è compromessa e farà davvero notizia.

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

Commenti dei lettori

