

CRYPTO-GRAM
15 settembre 2009

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

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

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

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

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

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

Crypto-Gram è anche consultabile in formato RSS.

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

In questo numero:

- Ottavo anniversario dell'11 settembre
- Novità su Skein
- Controllo degli accessi nel mondo reale
- News
- La cancellazione dei file
- Sulle telecamere di sorveglianza a Londra
- Gli alibi di Robert Sawyer
- Le news su Schneier
- Rubare 130 milioni di numeri di carte di credito
- "Il culto di Schneier"
- Commenti dei lettori

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

Ottavo anniversario dell'11 settembre

Il 30 settembre 2001 pubblicai un numero speciale di Crypto-Gram che trattava degli attacchi terroristici. Parlai della novità di quegli attacchi, di sicurezza aeroportuale, di analizzare dove e come aveva fallito l'intelligence, del potenziale di regolamentare la

crittografia -- perché potrebbe venire utilizzata dai terroristi -- e di proteggere la privacy e la libertà. Molto di quel che scrissi ha ancora rilevanza oggi.

<<http://www.schneier.com/crypto-gram-0109a.html>>

Un mio intervento del 2006: "Rifiutate di farvi terrorizzare".

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

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

Novità su Skein

Skein è uno dei 14 candidati SHA-3 selezionati dal NIST e promossi al secondo turno. Come parte del processo, il NIST ha concesso agli ideatori degli algoritmi di implementare piccoli 'aggiustamenti' ai loro algoritmi. Noi abbiamo agito sulle costanti di rotazione di Skein.

Lo studio su Skein revisionato contiene queste nuove costanti di rotazione, insieme a informazioni su come sono state scelte e perché sono state modificate, ai risultati di nuove crittanalisi, più nuovi vettori di inizializzazione e vettori di prova.

Le modifiche andavano eseguite entro la data in cui scrivo, 15 settembre. Ora il processo SHA-3 passa al secondo turno. Secondo la tabella cronologica del NIST, l'istituto selezionerà un gruppo di algoritmi 'finalisti' nel 2010, e un unico algoritmo hash nel 2012. Da qui a quel momento sta a tutti noi valutare gli algoritmi e far sapere al NIST quel che vogliamo. La crittanalisi è importante, naturalmente, ma lo sono anche le prestazioni.

Gli algoritmi promossi al secondo turno sono: BLAKE, Blue Midnight Wish, CubeHash, ECHO, Fugue, Grøstl, Hamsi, JH, Keccak, Luffa, Shabal, SHAvite-3, SIMD e Skein. Allo Zoo SHA-3 (vedere link più sotto) potete trovare informazioni approfondite su ognuno di essi, nonché sullo stato attuale della loro crittanalisi.

Per passare a notizie più leggere, stiamo anche producendo magliette a tema Skein. Chi di voi ha partecipato alla prima Hash Function Candidate Conference a Leuven in Belgio avrà notato le particolari ed eleganti polo nere indossate dal team Skein. Per chi ne volesse una, ora è possibile acquistarle. Tutti gli ordini devono essere ricevuti entro il primo ottobre, e produrremo tutte le magliette in un'unica partita.

Il sito Web di Skein:

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

Lo studio su Skein revisionato:

<<http://www.schneier.com/skein.pdf>>

Il codice sorgente di Skein revisionato:

<<http://www.schneier.com/code/skein.zip>>

Il mio articolo su SHA-3 del 2008:

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

Informazioni sulle magliette Skein:

<<http://www.schneier.com/skein-shirts.html>>

Il sito del NIST su SHA-3:

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

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

Lo Zoo SHA-3:

<http://ehash.iaik.tugraz.at/wiki/The_SHA-3_Zoo>

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

Controllo degli accessi nel mondo reale

Il controllo degli accessi è difficile in un contesto aziendale. Da una parte, ogni impiegato ha bisogno di un livello di accesso sufficiente per fare il proprio lavoro. Dall'altra, ogni volta che si concede un accesso maggiore a un impiegato i rischi aumentano: egli potrebbe abusare di tale accesso, o perdere informazioni a cui ha accesso, o essere indotto -- grazie a un'operazione di ingegneria sociale -- a offrire tale accesso a un individuo disonesto. Pertanto, un'azienda intelligente e previdente darà a ogni impiegato l'esatto livello di accesso che necessita per svolgere il proprio lavoro, né maggiore né minore.

Negli ultimi anni, sono state spese molte energie nel cosiddetto controllo degli accessi basato sul ruolo. Però, malgrado il gran numero di studi accademici e di prodotti di sicurezza di alto profilo, la maggior parte delle organizzazioni non lo implementa affatto, con tutti i prevedibili problemi di sicurezza che ne conseguono.

Capita di leggere regolarmente storie di dipendenti che abusano dei loro privilegi di controllo accessi di un database per motivi personali: registri sanitari, fiscali, anagrafici, penali. Gli intercettatori della NSA spiano le proprie mogli e fidanzate. Impiegati licenziati sottraggono segreti aziendali, e così via.

Un incidente spettacolare che riguarda il controllo accessi è accaduto nel Regno Unito nel 2007. Un impiegato del Fisco e Dogane di Sua Maestà (Her Majesty's Revenue & Customs) doveva inviare al National Audit Office duemila archivi di esempio estratti dal database del registro nazionale di tutti i bambini. Ma per quell'impiegato era più semplice copiare l'intero database di 25 milioni di persone in un paio di dischi e spedirli per posta anziché selezionare soltanto i le registrazioni richieste. Disgraziatamente i dischi sono andati perduti dalle poste e la faccenda è stata di grande imbarazzo per il governo.

Eric Johnson della Dartmouth's Tuck School of Business ha studiato a lungo il problema e i suoi risultati non stupiscono se si è riflettuto sul problema. È molto difficile istituire correttamente un controllo degli accessi basato sul ruolo. In genere le compagnie non riescono a determinare chi è in possesso di quale ruolo. Il dipendente non lo sa, il capo non lo sa -- e di questi tempi è assai frequente che un impiegato abbia più di un superiore -- e la direzione amministrativa di certo non lo sa. Vi è un motivo per cui il

controllo degli accessi basato sul ruolo (RBAC) proviene dal mondo militare: in quella realtà le strutture di comando sono semplici e ben delineate.

A peggiorare le cose, i ruoli cambiano rapidamente e in continuazione: Johnson ha tenuto traccia di un gruppo commerciale di 3.000 persone che ha sperimentato 1.000 cambi di ruolo nel giro di tre mesi soltanto. E spesso non è facile prevedere che tipo di informazioni occorrono a un dipendente fino a quando non ne ha effettivamente bisogno. E i dati stessi non sono così granulari. Così come è molto più semplice concedere l'accesso a un intero schedario che non alle singole cartelle di cui l'impiegato ha bisogno, è molto più semplice fornirgli l'accesso a un intero database che non ai singoli record di cui necessita.

Il risultato è che le imprese aumentano o restringono il raggio d'azione dei dipendenti, conferendo loro troppi o troppo pochi privilegi. Ma dato che terminare il lavoro è la cosa più importante, le aziende tendono a concedere troppi permessi. Johnson stima che dal 50 al 90% degli impiegati di grandi imprese possiedono più privilegi del necessario. Nel caso infrequente in cui un impiegato abbia necessità di accedere a informazioni alle quali normalmente non potrebbe, di solito esiste una qualche procedura che gli permette di ottenere l'accesso. E tale accesso, una volta garantito, non viene quasi mai revocato. In certe grandi aziende formali, Johnson ha potuto stabilire per quanto tempo un impiegato aveva lavorato lì basandosi sostanzialmente su quanto accesso disponeva.

Chiaramente, le aziende possono fare di meglio. Il compito attuale di Johnson è realizzare sistemi di controllo accessi con una semplice modalità di estensione dei privilegi quando necessario, con un sistema di auditing per garantire che non vi siano abusi di privilegi, con sanzioni in caso di violazioni (Intel, per esempio, punisce i trasgressori con 'multe' che seguono la logica delle multe per eccesso di velocità) e ricompense per il rispetto delle norme. Il suo obiettivo è ricavare il giusto insieme di incentivi e controlli per gestire gli accessi in maniera più adeguata, senza che le persone diventino troppo avverse ai rischi.

Alla fin fine, è semplicemente impossibile creare un sistema perfetto per il controllo degli accessi: c'è troppo caos nelle imprese perché funzioni. Ogni buon sistema dovrebbe permettere eventuali violazioni del controllo degli accessi, se vengono commesse in buona fede da persone che stanno solo cercando di fare il proprio lavoro. L'analogia con le multe per eccesso di velocità è migliore di quanto sembri a prima vista: si stabiliscono limiti di velocità di 55 miglia orarie, ma generalmente le multe vengono date a chi supera le 70 in quanto sussiste una certa tolleranza.

Questo articolo è stato originariamente pubblicato su Information Security, come parte di un 'botta e risposta' con Marcus Ranum. Potete leggere la risposta di Marcus a questo indirizzo, non prima di aver risposto a una serie di domande un po' indiscrete per poter ottenere un account gratuito.

<http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1365957_mem1,00.html>

oppure <<http://tinyurl.com/m7qhf4>>

Controllo degli accessi basato sul ruolo:

<http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1257133_mem1,00.html>

oppure <<http://tinyurl.com/n5mjmx>>

<[http://technet.microsoft.com/en-us/library/cc780256\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc780256(WS.10).aspx)>
<http://csrc.nist.gov/groups/SNS/rbac/documents/design_implementation/Intro_role_based_access.htm>
oppure <<http://tinyurl.com/ku8vnd>>
<<http://csrc.nist.gov/groups/SNS/rbac/documents/ferraiolo-kuhn-92.pdf>>

Abusi di accesso ai database:

<<http://articles.latimes.com/2009/may/09/local/me-hospital9>>
<<http://www.marketwatch.com/story/irs-worker-snooped-on-tax-records-of-almost-200-celebrities>>
oppure <<http://tinyurl.com/mrh7a8>>
<<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9115297>>
oppure <<http://tinyurl.com/mwr9je>>
<<http://rawstory.com/08/news/2009/06/18/reporter-nsa-analysts-spied-on-own-wives-and-girlfriends/>>
oppure <<http://tinyurl.com/mbgmw3>>
<<http://www.thetechherald.com/article.php/200924/3849/Trust-still-an-issue-in-IT-as-insiders-abuse-access-rights>>
oppure <<http://tinyurl.com/mk3lyf>>
<http://searchsecurity.techtarget.co.uk/news/article/0,289142,sid180_gci1318850,00.html>
oppure <<http://tinyurl.com/mu5ovb>>

L'incidente accaduto nel Regno Unito:

<<http://www.hmrc.gov.uk/news/hartnett-poynter-icc.htm>>
<http://news.bbc.co.uk/2/hi/uk_news/politics/7103566.stm>
<<http://www.computerweekly.com/Articles/2008/06/27/231267/hmrc-left-the-door-open-to-data-loss.htm>>
oppure <<http://tinyurl.com/mdqvm9>>

Il lavoro di Johnson:

<<http://mba.tuck.dartmouth.edu/digital/Research/ResearchProjects/DataFinancial.pdf>>
oppure <<http://tinyurl.com/ln4vhr>>
<<http://weis2008.econinfosec.org/papers/Zhao.pdf>>
<http://mba.tuck.dartmouth.edu/digital/Research/ResearchProjects/wise_v1.pdf>
oppure <<http://tinyurl.com/mtgsq2>>

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

News

Flash incorpora gli equivalenti dei cookie, ed è difficile eliminarli.

<<http://www.wired.com/epicenter/2009/08/you-deleted-your-cookies-think-again/>>
oppure <<http://tinyurl.com/l2qqaz>>

Allarme minaccia da trama cinematografica: robot dinamitardi suicidi. Brr, che paura.

<<http://www.telegraph.co.uk/news/newstopics/politics/lawandorder/6028144/Robot-suicide-bombers-fear.html>>
oppure <<http://tinyurl.com/orxxuz>>

Sono certo di aver visto cose del genere nei film.

È possibile falsificare prove del DNA:

<<http://arstechnica.com/science/news/2009/08/dna-samples-used-by-crime-labs-faked-in-research-lab.ars>>

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

<<http://www.nytimes.com/2009/08/18/science/18dna.html>>

<[http://www.fsigenetics.com/article/S1872-4973\(09\)00099-4/abstract](http://www.fsigenetics.com/article/S1872-4973(09)00099-4/abstract)>

Il termine legale "minacce terroristiche" è precedente alla tragedia dell'11 settembre, ma di questi tempi produce una reazione emotiva eccessiva:

<http://www.schneier.com/blog/archives/2009/08/the_continuing_2.html>

Sviluppi interessanti nella rilevazione della menzogna:

<http://www.scientificamerican.com/article.cfm?id=the-load-of-lying&sc=WR_20090804>

oppure <<http://tinyurl.com/njnn3o>>

Marc Webar Tobias su come hackerare la serratura Assa Solo:

<<http://www.thesidebar.org/insecurity/?p=447>>

Il mio intervento su serrature e relativi scassinamenti:

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

Dal sito di satira Cracked: "I 5 errori più imbarazzanti nella storia del terrorismo". Sì, molto divertente, ma ricordate che questi sono le grandi menti organizzative del terrorismo che i politici descrivono per tenerci spaventati.

<http://www.cracked.com/article/79_the-5-most-embarrassing-failures-in-history-terrorism/>

oppure <<http://tinyurl.com/lt68pa>>

Rilevante anche il mio articolo del 2007, "Ritratto del Terrorista Moderno da Idiota", ma meno divertente.

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

Modellazione di attacchi zombie: la matematica non è confortante. "When Zombies Attack!: Mathematical Modelling of an Outbreak of Zombie Infection" [Quando attaccano gli zombie: modelli matematici della propagazione di un'infezione zombie].

<<http://www.mathstat.uottawa.ca/~rsmith/Zombies.pdf>>

Pare che il lancio di una moneta non garantisca tutta questa casualità:

<<http://www.codingthewheel.com/archives/the-coin-flip-a-fundamentally-unfair-proposition>>

oppure <<http://tinyurl.com/d9kqt7>>

<<http://www-stat.stanford.edu/~susan/papers/headswithJ.pdf>>

Come parte del loro addestramento, gli agenti federali eseguono simulazioni in luoghi pubblici, a volte coinvolgendo civili innocenti. È tutta una messinscena di sicurezza.

<<http://www.washingtonpost.com/wp-dyn/content/article/2009/08/16/AR2009081602250.html?hpid=artslot&sid=ST2009081602301>>

oppure <<http://tinyurl.com/qd6zzz>>

<<http://www.startribune.com/59017377.html?elr=KArksUUUoDEy3LGDiO7aiU>>

Il genere di reati che abbiamo visto commettere ai danni di singoli individui iniziano ora a essere commessi ai danni di piccole aziende. Il problema è destinato a peggiorare, e grazie alle esternalità legate alla sicurezza, alle banche importerà molto meno.
<http://www.schneier.com/blog/archives/2009/08/small_business.html>

Un video interessante che dimostra come un agente di polizia possa alterare i risultati di un Breathalyzer (misuratore del tasso alcolico).
<<http://www.bing.com/videos/search?q=Breath+tests&qs=n&docid=992451363282&mid=AC91324DD782741BE4F2AC91324DD782741BE4F2&FORM=VIVR30#>>
oppure <<http://tinyurl.com/kkq8dk>>

Esiste un movimento nel Regno Unito che mira a far sostituire i boccali di vetro nei pub con boccali di materiale plastico, perché vengono usati troppo spesso come armi improprie. Non credo che questa iniziativa servirà a qualcosa, ma il livello di idiozia è impressionante. Mi ricorda dell'appello per vietare i coltelli appuntiti che, peraltro, anch'esso proveniva dal Regno Unito. Ma che succede laggiù?
<http://www.schneier.com/blog/archives/2009/08/banning_beer_gl.html>

Altre storie di sicurezza dal mondo della natura: vermi marini con bombe luminose:
<http://www.schneier.com/blog/archives/2009/08/marine_worms_wi.html>

Strano: "Il Federal Bureau of Investigation statunitense sta cercando di individuare chi spedisce computer portatili ai governatori di stato in tutto il paese, compresi il governatore della West Virginia Joe Mahchin e il governatore del Wyoming Dave Freudenthal. Alcuni funzionari statali temono che questi computer possano contenere software malevolo".

<<http://www.itworld.com/government/75885/fbi-investigating-laptops-sent-us-governors>>
oppure <<http://tinyurl.com/llf53a>>

L'affascinante vicenda di un phone phreaker sedicenne non vedente.
<http://www.rollingstone.com/news/story/29787673/the_boy_who_heard_too_much/p rint>
oppure <<http://tinyurl.com/nxnb9h>>

Sull'influenza porcina: "Dunque, pare che un virus che ha la possibilità non troppo remota di uccidere un essere umano necessiti di circa 25 kilobit, ossia 3,2 KB, di dati da codificare. Questo è molto più efficiente di un virus informatico, come MyDoom, che ha bisogno approssimativamente di 22 KB di dati. È umiliante che io possa venire ucciso da 3,2 KB di informazioni genetiche. Del resto, con 850 MB di dati nel mio genoma, è normale che esista qualche exploit".
<<http://www.bunniestudios.com/blog/?p=353>>

Un buon articolo sui timori esagerati per la guerra cibernetica:
<<http://bostonreview.net/BR34.4/morozov.php>>

Il vero rischio non è il terrorismo cibernetico, ma il crimine cibernetico.

SIGABA e la storia degli one-time pad:

<<http://www1.cs.columbia.edu/~smb/blog/control/>>

Parlai degli one-time pad, e della loro insicurezza pratica, nel 2002:

<<http://www.schneier.com/crypto-gram-0210.html#7>>

Discussione interessante sui mandati di comparizione come minaccia di sicurezza:
<<http://www.freedom-to-tinker.com/blog/felten/subpoenas-and-search-warrants-security-threats>>
oppure <<http://tinyurl.com/lwtdaz>>

Un'interessantissima intervista di un'ora a David Kilcullen sulla sicurezza e sull'insurrezione.
<<http://www.abc.net.au/unleashed/stories/s2668177.htm>>

La conferenza di Nils Gilman sull'economia illecita globale. Il Malware è uno degli esempi di Nils Gilman, a circa nove minuti dall'inizio del video.

<<http://video.google.com/videoplay?docid=3173247273890946684#>>

Le sette regole dell'economia illecita globale (durante il suo intervento, Gilman sembra utilizzare i termini 'illecito' e 'deviante' come sinonimi):

1. Forme di domanda perfettamente legittime possono produrre forme di offerta perfettamente devianti.
2. Strutture normative globali non omogenee creano opportunità di arbitraggio per imprenditori devianti.
3. I percorsi verso una globalizzazione legittima sono sempre anche percorsi verso una globalizzazione deviante.
4. Quando un'industria deviante si professionalizza, le misure restrittive non fanno altro che promuovere innovazione.
5. Gli stati medesimi compromettono la distinzione fra economia legittima e deviante.
6. Imprenditori devianti incontrollati supereranno l'economia legittima.
7. La globalizzazione deviante presenta una sfida esistenziale alla legittimità statale.

Intercettazioni della NSA perfettamente legali (ottenute con un mandato FISA) utilizzate per arrestare i dinamitardi con esplosivi liquidi.

<http://www.schneier.com/blog/archives/2009/09/nsa_intercepts.html>

La BBC ha una dimostrazione video in cui si vede una bottiglia da mezzo litro circa di esplosivo liquido che provoca una falla nella fusoliera di un aereo. Non conosco niente più di ciò che si vede sul video.

<http://news.bbc.co.uk/2/hi/uk_news/7536167.stm>

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

La cancellazione dei file

La cancellazione dei file è tutta una questione di controllo. Una volta non era un problema: i dati si trovavano nei nostri computer, ed eravamo noi a decidere quando e come eliminare un file. Potevamo servirci della funzione di cancellazione se non ci importava che il file potesse essere recuperato o meno, oppure un programma apposito per l'eliminazione dei file (io uso BCWipe per Windows) se volevamo garantire la totale irrecuperabilità del file.

Più spostiamo i nostri dati verso piattaforme di cloud computing come Gmail e Facebook, e verso piattaforme chiuse e proprietarie come Kindle e iPhone, cancellare i dati diventa più arduo.

Quando chiediamo a queste aziende di eliminare i nostri dati, dobbiamo fidarci che lo facciano, ma in genere non hanno interesse a farlo. Siti come quelli citati è più probabile che rendano le informazioni inaccessibili che non cancellarle fisicamente. Facebook è un colpevole riconosciuto sotto questo aspetto: l'effettiva eliminazione dei propri dati dai suoi server richiede una procedura complicata che potrebbe funzionare oppure no. E anche se riusciamo a cancellare le nostre informazioni, ne rimarranno sicuramente delle copie nei sistemi di backup dell'azienda. Gmail dice esattamente questo nella sua nota sulla privacy.

Backup online, messaggi SMS, fotografie su siti di condivisione di foto, applicazioni per smartphone che registrano i nostri dati nella rete: non abbiamo idea di quel che accade realmente quando cancelliamo certi dati o un intero account, perché non esercitiamo nessun controllo sui computer nei quali i dati sono conservati.

Questo concetto di controllo spiega inoltre come Amazon sia riuscita a cancellare un libro che gli utenti avevano precedentemente acquistato e caricato sui loro Kindle. L'aspetto legale si può discutere, ma indubbiamente Amazon ha avuto la possibilità tecnica di cancellare il file perché controlla tutti i Kindle. Ha progettato il Kindle in modo che determini quando aggiornare il software, se gli utenti hanno il permesso di acquistare libri per il Kindle, e quando disattivare completamente i Kindle degli utenti.

Vanish è un progetto di ricerca di Roxana Geambasu e di un team di suoi colleghi dell'Università di Washington. Hanno ideato un sistema prototipo che elimina automaticamente i dati dopo un intervallo di tempo prefissato. È quindi possibile inviare un'email, creare un documento in Google Docs, pubblicare una nota in Facebook o caricare una foto su Flickr, tutte informazioni destinate a scomparire dopo un periodo di tempo prestabilito. E dopo la sparizione di questi dati, nessuno -- né chi ha scaricato i dati, né il sito che li ha ospitati, né chiunque li abbia intercettati in transito, nemmeno noi stessi -- sarà in grado di leggerli. Se la polizia entrasse nelle sedi di Facebook, Google, o Flickr con un mandato, non sarà comunque in grado di recuperare quei dati.

I dettagli sono complessi, ma in sostanza Vanish spezza la chiave di decodifica dei dati in una serie di frammenti e li sparpaglia nel Web mediante una rete peer-to-peer. Poi sfrutta il movimento naturale di queste reti (il flusso di macchine che costantemente si collega e poi scollega) per far sparire i dati. A differenza di programmi precedenti che supportavano la cancellazione dei file, questo non richiede all'utente di fidarsi di qualche altra compagnia, azienda o sito Web. Cancella e basta.

Ovviamente Vanish non impedisce al destinatario di un'email o al lettore di una pagina di Facebook di copiare i dati e incollarli in un altro file, così come la funzione di eliminazione del Kindle non impedisce agli utenti di copiare i file di un libro e registrarli sui propri computer. Vanish è soltanto un prototipo a questo punto, e funziona solamente se tutte le persone che leggono i nostri aggiornamenti su Facebook o che guardano le nostre foto su Flickr lo installano sui loro computer; ma è una buona dimostrazione di come il controllo influisca sull'eliminazione dei file. E malgrado sia un passo nella direzione giusta, è anche una cosa nuova e deve essere sottoposta a ulteriori analisi di sicurezza prima di venire adottata su vasta scala.

Abbiamo perso il controllo dei dati su alcuni dei computer che possediamo, e abbiamo perso il controllo dei dati nella 'nuvola'. Non smetteremo di usare Facebook e Twitter solo perché queste aziende non cancelleranno i nostri dati quando glielo richiederemo, e non smetteremo di usare i Kindle e gli iPhone perché c'è la possibilità che cancellino i

nostri dati quando non vogliamo. Ma dobbiamo riprendere il controllo dei dati nella 'nuvola', e progetti come Vanish dimostrano che possiamo farlo.

Ora abbiamo bisogno di qualcosa che protegga i nostri dati quando una grande azienda decide di eliminarli.

Questo articolo è originariamente apparso sul Guardian.

<<http://www.guardian.co.uk/technology/2009/sep/09/bruce-schneier-file-deletion>>
oppure <<http://tinyurl.com/m9k2cm>>

BCWipe:

<<http://www.jetico.com/data-protection-wiping-bcwipe-enterprise/>>

Il mio intervento sul cloud computing:

<<http://www.schneier.com/essay-274.html>>

iPhone e il controllo:

<<http://www.schneier.com/essay-204.html>>

Le aziende di social networking non vogliono eliminare i dati:

<<http://www.schneier.com/essay-278.html>>

Come eliminare il vostro account Facebook:

<<http://www.wikihow.com/Permanently-Delete-a-Facebook-Account>>

Kindle:

<<http://bit.ly/KindleDelete>>

<<http://www.techdirt.com/articles/20090416/0246064526.shtml>>

Vanish:

<http://www.economist.com/sciencetechnology/tm/displaystory.cfm?story_id=14162535>

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

<<http://vanish.cs.washington.edu/index.html>>

<<http://vanish.cs.washington.edu/pubs/usenixsec09-geambasu.pdf>>

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

Sulle telecamere di sorveglianza a Londra

Un resoconto recente ha concluso che le telecamere di sorveglianza di Londra hanno risolto un crimine su mille telecamere, per anno.

Non ho esaminato il resoconto, ma so che è difficile stabilire quando un crimine sia stato 'risolto' da una telecamera di sorveglianza. Per come la vedo io, quel crimine deve per forza essere stato irrisolvibile senza le telecamere. Non posso fare a meno di notare come i sostenitori delle telecamere portino sempre l'esempio delle immagini delle telecamere di sorveglianza che hanno identificato i dinamitardi che hanno colpito i servizi di trasporto pubblico a Londra il 7 luglio, ma è ovvio che i dinamitardi sarebbero stati identificati anche senza l'apporto delle telecamere.

E conoscere che genere di crimini sono stati 'risolti' dalle telecamere mi aiuterebbe davvero a capire le ventimila sterline annue costate per telecamera (calcolate prendendo la spesa iniziale di 200 milioni di sterline per l'acquisto delle telecamere moltiplicato 1 su 1000 telecamere utilizzate per risolvere un crimine all'anno diviso per dieci anni). Se i 200 milioni di sterline sono serviti a risolvere 10.000 omicidi, potrebbe benissimo trattarsi di un ottimo compromesso di sicurezza. Ma immagino che la maggior parte di quei crimini fossero di caratura assai minore.

<http://news.bbc.co.uk/2/hi/uk_news/england/london/8219022.stm>
<<http://www.telegraph.co.uk/news/uknews/crime/6082530/1000-CCTV-cameras-to-solve-just-one-crime-Met-Police-admits.html>>
oppure <<http://tinyurl.com/nblfwd>>

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

Gli alibi di Robert Sawyer

Nel 2002, l'autore di fantascienza Robert J. Sawyer scrisse un saggio sul compromesso fra privacy e sicurezza. Non ho mai dimenticato la prima frase: "Ogni volta che vado a visitare un'attrazione turistica dove è presente un registro degli ospiti, metto sempre la mia firma. Dopotutto non si sa mai quando si può aver bisogno di un alibi".

Da quando ho letto quel saggio, ogni volta che vedo un'attrazione turistica con un registro degli ospiti, faccio la stessa cosa. Firmo: "Robert J. Sawyer, Toronto, Ontario" - - perché non si sa mai quando lui avrà bisogno di un alibi.

Il saggio di Sawyer:
<<http://sfwriter.com/privacy.htm>>

Alcuni dei miei interventi sulla privacy:
<<http://www.schneier.com/essay-109.html>>
<http://www.schneier.com/blog/archives/2006/05/the_value_of_pr.html>
<<http://www.schneier.com/essay-261.html>>

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

Le news su Schneier

Interverrò all'Università del Kentucky il 17 settembre.
<<http://www.cs.engr.uky.edu/events/distingLectures.php>>

Interverrò anche al II International Symposium on Network and Data Communications, a Lima, in Peru il 25 settembre.
<<http://www.tecsup.edu.pe/simposio09/redes/preventaingles.html>>

E interverrò al GOVCERT.NL a Rotterdam il 6 ottobre.

<https://www.govcert.nl/symposium/index.html>

Qui potete trovare il video di una conferenza, "The Future of the Security Industry" [Il futuro dell'industria della sicurezza], che ho tenuto a un meeting OWASP ad agosto a Minneapolis.

<<http://vimeo.com/6495257>>

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

Rubare 130 milioni di numeri di carte di credito

Qualcuno è stato accusato di aver rubato 130 milioni di numeri di carte di credito.

Sì, è una bella cifra, ma è l'ordine di grandezza in cui si trovano i numeri di carte di credito. Ve ne sono miliardi registrati in grossi file database. Anche se volete rubarne solo dieci, dovrete rubarne a milioni. Sono certo che ognuno di noi ha una carta di credito nel portafoglio il cui numero è stato rubato. Con ogni probabilità non verrà mai utilizzato a scopi fraudolenti, ma si trova comunque da qualche parte in un database rubato.

Anni fa, nel dare consigli su come evitare il furto di identità, avrei detto alle persone di distruggere la spazzatura. Oggi un suggerimento del genere è totalmente obsoleto. Nessuno più ruba numeri di carta di credito andando a frugare nella spazzatura quando può rubarne a milioni da qualche database commerciale.

<http://news.yahoo.com/s/ap/20090817/ap_on_re_us/us_hacker_charges>

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

"Il culto di Schneier"

Se un culto del genere esiste davvero, fatemi sapere. In un saggio così intitolato, John Viega parla dei rischi che si incorre affidandosi sul mio libro "Applied Cryptography" per progettare sistemi crittografici:

"Ma, dopo molti anni passati a valutare la sicurezza dei sistemi informatici, sono veramente restio a servirmi del libro che ha reso Bruce famoso quando si tratta di progettare gli aspetti crittografici di un sistema. Infatti posso dire con certezza che non ho mai visto un sistema sicuro quando [Applied Cryptography] è stata la fonte primaria del design crittografico. E con questo non voglio dire che la gente si dimentica dei buffer overflow, ma proprio che la parte crittografica è pessima.

"La regola che impartisco ai team di sviluppo software è semplice: non usate Applied Cryptography nella progettazione del vostro sistema. È una lettura ottima e divertente, ma non utilizzatela come fondamento per un progetto.

[...]

“Il libro parla dei mattoni fondamentali della crittografia, ma non vi è alcuna guida costruttiva per mettere insieme tutti quei mattoni allo scopo di creare una connessione sicura e autenticata fra due parti.

“Inoltre, nei 13 anni circa passati dall’ultima revisione del volume, la nostra comprensione della crittografia è cambiata sensibilmente. Il libro contiene cose che si ritenevano vere a quel tempo, e che si sono rivelate completamente false...

Sono d’accordo. E, bisogna dargliene atto, Viega stesso fa notare che io concordo:

“Ma nell’introduzione del libro ‘Practical Cryptography’ di Bruce Schneier, egli stesso sostiene che il mondo è pieno di sistemi malfatti creati partendo dal suo precedente volume. Infatti Schneier ha scritto ‘Practical Cryptography’ nella speranza di sistemare il problema”.

È tutto vero.

Progettare un sistema crittografico è difficile. Così come non dareste a nessuno, neanche a un medico, un manuale di istruzioni di neurochirurgia e poi pretendere che questi operi su pazienti veri, non dovrete dare a un ingegnere un libro sulla crittografia e poi pretendere che progetti e implementi un sistema crittografico. È assai improbabile che il paziente sopravviva, come è assai improbabile che il sistema crittografico sia sicuro.

Ancora peggio, la sicurezza non offre un feedback immediato. Un paziente morto sul lettino della sala operatoria è un chiaro risultato che dice al medico che forse non conosce bene la neurochirurgia solo perché ha letto un libro. Ma un sistema crittografico non sicuro funziona lo stesso. È solo quando qualcuno si prende la briga di comprometterlo che l’ingegnere potrà rendersi conto che non ha fatto il gran lavoro che credeva. Ricordate: chiunque è in grado di progettare un sistema di sicurezza che non è in grado di battere. Anche gli esperti sbagliano regolarmente. Le probabilità che un dilettante riesca nell’impresa sono estremamente basse.

Per chi fosse interessato, verrà pubblicata nel 2010 una seconda edizione di ‘Practical Cryptography’, che si intitolerà ‘Cryptography Engineering’ e avrà un terzo autore: Tadayoshi Kohno.

<<http://broadcast.oreilly.com/2009/01/the-cult-of-schneier.html>>

Applied Cryptography:
<<http://www.schneier.com/book-applied.html>>

Practical Cryptography:
<<http://www.schneier.com/book-practical.html>>

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

Commenti dei lettori

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

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

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

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

La versione italiana è curata da Communication Valley SpA
<<http://www.communicationvalley.it/>>

Per iscriversi o cancellarsi andare all'indirizzo <<http://www.cryptogram.it/>>
I numeri arretrati sono disponibili all'indirizzo <<http://www.cryptogram.it/>>
Per informazioni <crypto-gram@communicationvalley.it>

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

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

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

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

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

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

Copyright (c) 2009 - Bruce Schneier.