

CRYPTO-GRAM
15 dicembre 2008

Scritta da Bruce Schneier
Fondatore e CTO di BT Counterpane

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:

Lezioni apprese dai fatti di Mumbai
Le comunicazioni durante attacchi terroristici NON SONO una cosa negativa
I terroristi di Mumbai si sono serviti di Google Earth, di barche, di cibo...
L'auditing
News
Il futuro delle conversazioni effimere
Recensione di "Here Comes Everybody"
Le news su Schneier/BT Counterpane
L'FBI alimenta paure
Schneier amministratore della TSA?
Notizie su Skein e SHA-3
Commenti dei lettori

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

Lezioni apprese dai fatti di Mumbai

Scritto immediatamente dopo la strage:

Mi sto ancora informando sugli attacchi terroristici di Mumbai, e immagino passerà del tempo prima che si sapranno molti dettagli. Ciò che sappiamo al momento è tremendo, e la mia solidarietà va ai sopravvissuti alla strage (e ai feriti, che pare vengano spesso ignorati con tutta l'attenzione del pubblico rivolta al bilancio delle vittime). Senza voler minimizzare la tragicità degli eventi, queste sono le mie osservazioni iniziali:

* La 'bassa tecnologia' è assai efficace. La gente si preoccupa di minacce da trama cinematografica (terroristi muniti di polverizzatori agricoli, terroristi con agenti biologici, terroristi che prendono di mira le nostre riserve d'acqua), ma in realtà è bastato un gruppo di uomini addestrati (non sappiamo ancora che genere di addestramento hanno ricevuto, ma è evidente che ne abbiano ricevuto uno) con armi da fuoco e granate.

* Allo stesso tempo, gli attacchi hanno fatto registrare un numero di morti sorprendentemente basso. Non riesco a trovare le cifre precise, ma pare che vi fossero circa 18 terroristi. Il bilancio delle vittime più recente parla di 195 morti e 235 feriti. Equivale a 11 morti e 13 feriti per terrorista. Per terribile che sia la realtà, si tratta di numeri molto più bassi rispetto a quelli che avreste previsto se vi foste immaginati il film scorrere nella vostra testa. La realtà è diversa dai film.

* E in ogni caso, il terrorismo è un fenomeno raro. Se basta davvero un gruppo di uomini con pistole e granate, perché questo genere di terrorismo non è più diffuso? E perché non avviene negli Stati Uniti, dove è più facile entrare in possesso di armi? È perché il terrorismo è davvero molto raro.

* Misure di sicurezza specifiche non servono con questo tipo di attacchi. Nessuna delle costose contromisure che proteggono da tattiche e bersagli specifici è servita, o sarebbe servita, a molto: controllare documenti con foto, confiscare liquidi negli aeroporti, prendere le impronte digitali degli stranieri alle frontiere, controllare i bagagli sui mezzi pubblici, qualunque cosa. Persino i metal detector e gli allarmi terrorismo non sono serviti a nulla.

Se c'è una lezione da apprendere da questi attacchi, è quella di non concentrarsi troppo sulle particolarità degli attacchi. Ovviamente non è il modo in cui siamo programmati a pensare. Di solito reagiamo alle storie, non all'analisi. Non voglio sembrare distaccato: una simile tendenza è umana e tutte quelle morti sono una vera tragedia. Ma 18 individui armati e con l'intenzione di uccidere moltissimi innocenti riusciranno nel loro intento e le contromisure da ultima spiaggia non saranno certo in grado di fermarli. Come sempre: intelligence, indagini e risposta alle emergenze. Dobbiamo scovare e fermare i terroristi prima che attacchino, e gestire le conseguenze degli attacchi che non riusciamo a evitare. Non c'è altro modo, davvero, e mi auguro che non permetteremo a questa tragedia di portarci a prendere decisioni avventate su come affrontare il terrorismo.

<<http://www.news.com.au/couriermail/story/0,23739,24726093-954,00.html>>

<http://www.upi.com/Top_News/2008/11/29/Executive_says_Taj_hotel_warned_of_attack/UPI-97361228007685/>

oppure <<http://tinyurl.com/5onsh6>>

<<http://www.pebbleandavalanche.com/weblog/2008/11/30/blog-20081130T1857>>

Minacce da trama cinematografica:

<<http://www.schneier.com/essay-087.html>>

Il nostro cervello e altre storie:

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

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

Le comunicazioni durante attacchi terroristici NON SONO una cosa negativa

Twitter è stata una fonte di informazioni importantissima a Mumbai; in molti hanno utilizzato il servizio per comunicare e aggiornare gli altri durante gli attacchi terroristici. Dobbiamo semplicemente essere più brillanti di quest'idea: "E stamane gli utenti di Twitter hanno detto che le autorità indiane stavano chiedendo agli utenti di smettere di scrivere aggiornamenti, per motivi di sicurezza. Una persona ha scritto: 'La polizia ritiene che gli utenti di Twitter stiano rivelando informazioni strategiche ai terroristi attraverso il sito'".

Questa paura, in realtà, si muove nella direzione contraria. Durante un attacco terroristico (anzi, durante qualsiasi situazione di crisi), quel che può fare la gente è proprio scambiarsi informazioni. È di aiuto per le persone, le calma, e riduce proprio ciò che i terroristi stanno cercando di ottenere: il terrore. Certo, esistono particolari scenari da trama cinematografica in cui certe dichiarazioni pubbliche potrebbero aiutare i terroristi, ma sono eventi rari. Personalmente, preferisco eccedere in quanto a informazioni, apertura, e comunicazione in generale.

<http://technology.timesonline.co.uk/tol/news/tech_and_web/article5245059.ece>

oppure <<http://tinyurl.com/5zu8zc>>

<<http://stephensonstrategies.com/2008/11/26/us-officials-must-monitor-learn-from-use-of-web-20-in-mumbai/>>

oppure <<http://tinyurl.com/58htvy>>

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

I terroristi di Mumbai si sono serviti di Google Earth, di barche, di cibo...

I terroristi di Mumbai si sono serviti di Google Earth per pianificare i loro attacchi. Questo particolare disturba alcune persone:

"Google Earth è già stato oggetto di critiche in India, anche da parte dell'ex presidente del paese, A.P.J. Abdul Kalam.

"Durante una conferenza nel 2005 Kalam aveva fatto notare come la facile reperibilità su Internet di mappe dettagliate dei paesi del mondo, messe a disposizione da servizi come Google Earth, poteva essere sfruttata dai terroristi".

Ma è ovvio che i terroristi hanno utilizzato Google Earth. Si sono anche serviti di barche e hanno mangiato in ristoranti. Per non parlare del fatto che hanno persino respirato aria e bevuto acqua.

“Una portavoce di Google ha scritto in un’email giunta oggi che le immagini di Google Earth sono reperibili mediante fonti pubbliche e commerciali. Ha inoltre dichiarato che Google Earth è stato anche utilizzato da organizzazioni umanitarie durante operazioni di soccorso, e ciò ha molto più valore di qualsiasi uso abusivo”.

Questo è vero per qualunque aspetto dell’infrastruttura umana. Sì, viene utilizzata dai malviventi: i rapinatori di banche si servono di automobili per scappare, i contrabbandieri di droga usano le radio per comunicare, i pedopornografi fanno uso della posta elettronica. Ma anche le persone perbene si servono di queste cose, e gli usi legittimi superano in importanza quelli illeciti.

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=networking_and_internet&articleId=9121819&taxonomyId=16&intsrc=kc_to_p> oppure <<http://tinyurl.com/6sytye>>

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

L’auditing

Come primo presidente 'digitale', Barack Obama si sta rendendo conto sulla propria pelle quanto sia difficile mantenere la privacy nell’era dell’informazione. Agli inizi dell’anno alcuni impiegati a contratto del Dipartimento di Stato hanno curiosato nella documentazione relativa al suo passaporto. In ottobre, qualcuno all’ICE (Immigration and Customs Enforcement, l’agenzia del Dipartimento di Sicurezza Nazionale statunitense che si occupa di immigrazione) ha divulgato informazioni sullo stato di immigrazione di sua zia. E in novembre, alcuni dipendenti di Verizon hanno dato un’occhiatina ai registri delle sue telefonate cellulari.

Quel che dimostrano i tre incidenti menzionati non è tanto che i database computerizzati siano vulnerabili all’hacking -- questo lo sapevamo già, e comunque tutte quelle persone avevano un accesso legittimo ai sistemi che hanno utilizzato -- semmai illustrano l’importanza dell’auditing come misura di sicurezza.

Quando pensiamo alla sicurezza, di solito pensiamo a misure preventive: serrature che tengano alla larga i ladri dalle nostre case, cassette di sicurezza nelle banche per mettere al sicuro il nostro denaro, e screener negli aeroporti che evitino l’introduzione di armi e ordigni sugli aerei. Possiamo anche pensare a misure di rilevamento e di risposta: allarmi che si attivano quando i ladri forzano le serrature per entrare in casa nostra o quando fanno saltare le casseforti nelle banche, sky marshal sugli aerei che rispondono in caso un dirottatore riesca a superare la sicurezza aeroportuale portandosi a bordo una pistola. Ma l’auditing, ossia lo scoprire chi ha commesso cosa dopo il fatto, è spesso una misura di sicurezza molto più importante delle altre tre appena menzionate.

Il grosso della sicurezza contro i reati proviene dall’auditing. Naturalmente ci serviamo di serrature e di allarmi, ma non andiamo in giro indossando giubbetti antiproiettile. La polizia provvede alla nostra incolumità facendo indagini sui reati dopo i fatti e perseguendo i responsabili: questo è auditing.

L'auditing contribuisce a garantire che le persone non abusino di posizioni di fiducia. Il registratore di cassa, per esempio, è sostanzialmente un sistema di auditing. I cassieri devono maneggiare il denaro del negozio. Per fare in modo che non sottraggano soldi dalla cassa, il registratore di cassa tiene traccia di tutte le transazioni. Il proprietario del negozio può così controllare i totali alla fine della giornata e verificare che la quantità di denaro in cassa sia quella che dovrebbe essere.

Lo stesso concetto ci protegge anche dagli abusi delle forze dell'ordine. La polizia ha poteri molto vasti, fra cui la possibilità di invadere aspetti molto intimi della nostra vita allo scopo di risolvere crimini e mantenere pace e ordine. Ciò in genere è buona cosa, ma per fare in modo che la polizia non abusi di questo potere vengono creati dei sistemi di auditing come la procedura del mandato.

L'intero scandalo delle intercettazioni senza mandato della NSA riguarda proprio questo aspetto del problema. Alcuni, in maniera fuorviante, hanno descritto l'operazione come se fosse un'autorizzazione data al governo per intercettare le comunicazioni di terroristi stranieri, ma il governo ha sempre avuto quell'autorità. In realtà ciò che il governo voleva era evitare di presentare un mandato, anche dopo il fatto, a una FISA Court (Foreign Intelligence Surveillance) segreta. Ciò che il governo voleva era evitare di essere soggetto ad auditing.

E quella sarebbe un'idea incredibilmente pessima. I sistemi per il mantenimento dell'ordine privi di buone funzionalità di auditing incorporate, o che sono esenti da questo tipo di supervisione basata sull'auditing, sono molto più soggetti all'abuso da parte di chi ha potere -- perché tali individui possono abusare del sistema senza correre il rischio di essere scoperti. A mano a mano che l'opera di spionaggio nazionale della NSA aumenta, l'auditing è essenziale e necessario. E grandi database di polizia, come il Next Generation Identification System dell'FBI, devono assolutamente incorporare potenti funzioni di auditing.

Per sistemi di database computerizzati come quello -- sistemi a cui si affidano le informazioni di altre persone -- l'auditing è un meccanismo di sicurezza molto importante. Gli ospedali hanno bisogno di conservare database contenenti informazioni mediche molto personali, e dottori e infermieri devono poter accedere a tali informazioni in maniera semplice e rapida. Un buon registro di auditing che tenga traccia di chi ha consultato cosa e quando, è il sistema migliore per garantire che le persone a cui affidiamo le nostre informazioni mediche non abusino di tale fiducia. Stesso discorso per i registri fiscali, per gli estratti conto delle carte di credito, per i database di polizia e per i registri telefonici -- qualsiasi tipo di documentazione personale che qualcuno possa voler spiare durante il corso del suo lavoro.

Il che ci riporta al presidente Obama. In ognuno dei tre esempi visti prima, qualcuno in una posizione di fiducia ha inopportuno consultato informazioni personali. Le differenze fra i vari sistemi di auditing hanno determinato il corso delle conseguenze. L'auditing del Dipartimento di Stato è quel che ha funzionato meglio: vi erano dei sistemi di allarme che hanno allertato i superiori su quando la documentazione sul passaporto di Obama è stata consultata e su chi ha avuto accesso a tali informazioni. I meccanismi di auditing di Verizon non si sono comportati altrettanto bene: hanno scoperto l'accesso inopportuno all'account e hanno ristretto la lista dei sospettati ad alcune persone. L'auditing all'Immigration and Customs Enforcement non è stato molto efficace: ancora non si sa chi ha acceduto alle informazioni.

Vasti database pieni di informazioni personali, che siano gestiti da governi o da organizzazioni, sono un aspetto essenziale dell'era dell'informazione. E devono poter essere consultati, per scopi legittimi, da migliaia o da decine di migliaia di persone. L'unico modo per assicurarsi che quelle persone non abusino del potere loro affidato è attraverso l'auditing. Senza di esso non potremo mai sapere chi sta avendo accesso a cosa.

Storie su Obama:

<<http://www.cnn.com/2008/POLITICS/03/20/obama.passport/index.html>>
<<http://edition.cnn.com/2008/POLITICS/11/01/obama.aunt.ap/index.html>>
<<http://online.wsj.com/article/SB122724536331647671.html>>
<<http://arstechnica.com/news.ars/post/20080321-analysis-obamas-privacy-lesson-and-its-real-id-implications.html>>
oppure <<http://tinyurl.com/25ofv2>>
<http://www.usatoday.com/news/politics/election2008/2008-10-31-obama-aunt_N.htm> oppure <<http://tinyurl.com/6ddkbg>>

Lo spionaggio nazionale della NSA:

<<http://online.wsj.com/article/SB120511973377523845.html>>

Il Next Generation Identification System dell'FBI:

<<http://www.fbi.gov/pressrel/pressrel08/ngicontract021208.htm>>

Questo articolo è originariamente apparso sul sito del Wall Street Journal.

<<http://online.wsj.com/article/SB122877438178489235.html>>

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

News

Il volume di spam è diminuito di circa il 75% dopo che un solo provider di servizi di hosting è stato scollegato. Gli spammer stavano utilizzando quel provider per controllare la maggioranza degli spam bot zombie su Internet.

<http://voices.washingtonpost.com/securityfix/2008/11/spam_volumes_drop_by_23_after.html> oppure <<http://tinyurl.com/5hvrel>>

Il volume è tornato ai livelli normali nel giro di qualche settimana: gli spammer hanno trovato altre aziende di hosting per controllare le proprie operazioni.

La gente dice che tutti gli imbrogli si appoggiano sull'ingordigia della vittima per funzionare. Ma questo breve articolo sulla neuroscienza delle truffe lascia intendere che l'ingordigia sia soltanto un fattore secondario.

<<http://blogs.psychologytoday.com/blog/the-moral-molecule/200811/how-run-a-con>> oppure <<http://tinyurl.com/5aelyx>>

Charles Nesson, professore di legge ad Harvard sta sostenendo di fronte a un tribunale che il Digital Theft Deterrence and Copyright Damages Improvement Act del 1999 è anticostituzionale.

<<http://techdirt.com/articles/20081030/0203582685.shtml>>
<http://www.usatoday.com/tech/news/2008-11-16-music-downloading_N.htm>

Fuga di informazioni: divulgati gli indirizzi IP dei servizi segreti tedeschi:
<[http://wikileaks.org/wiki/German_Secret_Intelligence_Service_\(BND\)_T-Systems_network_assignments,_13_Nov_2008](http://wikileaks.org/wiki/German_Secret_Intelligence_Service_(BND)_T-Systems_network_assignments,_13_Nov_2008)> oppure <<http://tinyurl.com/66569b>>

Sky marshal che commettono reati:
<http://www.usatoday.com/news/washington/2008-11-12-air-marshals_N.htm>

Un compromesso di sicurezza: "Gli attivisti per la sicurezza dei bambini sostengono che alcune aziende che realizzano sistemi di verifica dell'età intendano aiutare altre compagnie su Internet a fornire annunci pubblicitari mirati ai bambini. Dicono che queste aziende stanno sostituendo una minaccia esagerata -- lo spettro dei predatori sessuali online -- con un pericolo ancor più pervasivo da parte di commercianti online, come le aziende produttrici di merendine e giocattoli, che si metteranno subito a inviare pubblicità ai bambini una volta che verranno a conoscenza delle giuste informazioni sugli utenti". È una vecchia storia: proteggersi contro eventi rari e spettacolari rendendosi più vulnerabili a ciò che è banale e comune.
<<http://www.nytimes.com/2008/11/16/business/16ping.html>>

Una cassaforte costruita con mattoncini Lego:
<<http://www.slipperybrick.com/2008/11/legos-safe/>>

Lo Smithsonian ha dovuto trovare un sistema per preservare un calamaro gigante conformandosi al tempo stesso con le regolamentazioni post-11 settembre sui materiali infiammabili:
<<http://pubs.acs.org/cen/science/86/8644sci1.html>>

Fuga di informazioni: divulgato un database contenente i nomi di membri del British National Party, partito di estrema destra:
<http://wikileaks.org/wiki/British_National_Party_membership_and_contacts_list%2C_2007-2008> oppure <<http://tinyurl.com/6cstze>>

Il governo può determinare la posizione dei telefoni cellulari senza assistenza da parte delle imprese di telecomunicazioni.
<<http://arstechnica.com/news.ars/post/20081116-foia-docs-show-feds-can-lojack-mobiles-without-telco-help.html>>
oppure <<http://tinyurl.com/5n4ush>>

Questa dichiarazione, fatta dalla persona scelta da Obama come capo del Dipartimento per la Sicurezza Nazionale, mi sorprende: "Il Governatore Janet Napolitano ha 'abbattuto' l'idea di costruire un muro di confine, affermando che sarebbe una spesa troppo costosa, che la sua edificazione impiegherebbe troppo tempo, e che sarebbe una misura inefficace una volta ultimato. 'Mostratemi un muro alto 50 piedi e io vi mostrerò una scala alta 51 piedi al confine. Ecco come funzionano le frontiere', Napolitano ha dichiarato alla Associated Press. Invece che nella costruzione di un muro, il Governatore ha detto che i fondi sarebbero meglio impiegati nell'aumentare il numero di agenti di pattuglia in frontiera, in sensori elettronici e in veicoli aerei robotizzati". Sono cautamente ottimista.
<http://www.worldnetdaily.com/news/article.asp?ARTICLE_ID=48017>

I college non stanno dando molti compiti a casa ultimamente; il concorso di Victoria's Secret viene sabotato.

<<http://media.www.dailypennsylvanian.com/media/storage/paper882/news/2008/11/21/News/Victoria.Secret.Competition.Gets.Hacked-3556689.shtml>> oppure

<<http://tinyurl.com/68t6se>>

Seriatamente, è difficile prevenire l'alterazione dei voti nei sondaggi online.

Cifrario 'carta e penna' del 1941:

<<http://www.slugsite.com/archives/957>>

Kit di sopravvivenza terroristica per Windows Mobile. Pare che non si tratti di uno scherzo.

<<http://www.microsoft.com/windowsmobile/catalog/product.aspx?catid=5&subid=22&bin=1&device=0&os=2&size=10&productid=006cdc5e-3094-4b4e-a3d2-2b5241ec4ec5>> oppure <<http://tinyurl.com/64756b>>

Avrei voluto partecipare alla Evolutionary Perspectives on War Conference (Conferenza sulle prospettive evolutive della guerra):

<http://www.uoregon.edu/~icds/Evolutionary_Perspectives_on_War_Conference_files/ProgramWeb.pdf> oppure <<http://tinyurl.com/56x2oa>>

Ecco uno studio sull'argomento pescato casualmente:

<<http://www.kuro5hin.org/story/2006/4/17/194059/296>>

In questa storia sul furto di bagagli al Los Angeles International Airport troviamo il seguente paragrafo, molto interessante: "Entrambi hanno detto che esistono cerchie organizzate di ladri, che individuano oggetti di valore nel bagaglio fatturato osservando gli schermi delle macchine a raggi X della TSA, poi comunicano con gli addetti ai bagagli via cellulare o SMS, dicendo loro che cosa cercare con esattezza". Qualcuno dovrebbe indagare fino a che punto le misure di sicurezza della TSA facilitino il crimine.

<<http://cbs2.com/local/Airport.Luggage.Thefts.2.858482.html>>

Sul mio blog:

<http://www.schneier.com/blog/archives/2008/12/tsa_aiding_lugg.html>

Questa è la storia di una donna che ha inviato 400.000 dollari ai truffatori nigeriani.

<<http://timesonline.typepad.com/technology/2008/11/this-woman-sent.html>>

<http://www.schneier.com/blog/archives/2008/12/who_falls_for_t.html#c328221>

oppure <<http://tinyurl.com/5b7ql9>>

L'idea alla base di una carta di credito con un generatore di password one-time è che riduce la frode di tipo 'carta non presente'. L'efficacia di questa contromisura dipende molto da quanto costano queste nuove carte di credito rispetto alla frequenza di tale frode, ma in generale sembra essere un'ottima idea. Sicuramente migliore del codice a tre cifre stampato sul retro delle carte. Secondo l'articolo, Visa collauderà questa nuova carta nel 2009 nel Regno Unito. Le banche dei Paesi Bassi è da molti anni che sono dotate di questo tipo di carta di credito.

<<http://www.dailymail.co.uk/sciencetech/article-1085642/The-new-credit-card-keypad-promises-fight-online-fraud.html?ITO=1490>>

oppure <<http://tinyurl.com/6jun7m>>

<https://bankieren.rabobank.nl/mijnbankzaken?ra_mfvars=clickout|Rabobank+-+Particulieren|externalwebsite>

oppure <<http://tinyurl.com/6drooh>>

È da un certo tempo che la NASA è vittima di attacchi cibernetici.

<http://www.businessweek.com/print/magazine/content/08_48/b4110072404167.htm

> oppure <<http://tinyurl.com/5gk747>>

Un detenuto evade spedendosi per posta fuori dalla prigione. Forse non si tratta di una tattica ovvia, e forse in un penitenziario vengono controllati con più cura i grossi pacchi in arrivo, piuttosto che quelli in uscita -- ma uno si aspetterebbe che le guardie facciano attenzione a qualsiasi pacco sufficientemente grande da contenere una persona.

<<http://news.bbc.co.uk/1/hi/world/europe/7730018.stm>>

Mi ricordo della visita ad Alcatraz che feci alcuni anni fa, e mi pare che la guida aveva parlato di qualcuno che tentò di evadere nascondendosi in un carrello della biancheria sporca. Per cui forse quest'idea non è poi così nuova.

Jeffrey Goldberg su come proteggersi dal terrorismo negli hotel. Fa notare che "il mio guru personale della sicurezza, Bruce Schneier, dice che è stupido preoccuparsi della propria incolumità negli alberghi perché le probabilità che succeda qualcosa in una certa notte in un certo albergo sono infinitamente piccole. Il tratto in taxi per andare in albergo è invariabilmente più pericoloso dell'albergo stesso". E lo ribadisco. Ma se di solito soggiornate in alberghi designati come bersaglio, i suoi consigli sono ottimi.

<http://jeffreycgoldberg.theatlantic.com/archives/2008/11/how_to_stay_alive_in_a_terrori.php> oppure <<http://tinyurl.com/5tuw7x>>

Elenco interessante di truffe ai danni dei turisti:

<http://www.ricksteves.com/graffiti/bestof_scams05.htm>

Questo studio, "Terrorism-Related Fear and Avoidance Behavior in a Multiethnic Urban Population" (Paura legata al terrorismo e condotta di evitamento in una popolazione urbana multi-etnica) è solo per abbonati. L'abstract è interessante però:

<http://www.schneier.com/blog/archives/2008/12/who_worries_abo.html>

Questo è un drive USB camuffato da pezzo di cavo tranciato. È sempre bene criptarlo, ma con ogni probabilità passerà inosservato se i vostri bagagli vengono controllati in dogana, se la polizia effettua una perquisizione a casa vostra, o se lo perdetevi.

<<http://www.thinkgeek.com/computing/drives/ab63/?cpg=81H>>

Ecco qualcuno che sostiene che sia "impossibile" hackerare termostati controllati via radio perché sono criptati. Certa gente proprio non comprende la sicurezza.

<<http://www.nytimes.com/2008/01/11/us/11control.html>>

Jim Harper risponde ai miei commenti sul prendere le impronte digitali agli stranieri alle frontiere.

<<http://techliberation.com/2008/11/12/border-biometrics-zero-benefit/>>

Lockheed Martin sta collaudando robot assassini:

<<http://www.thirdeyeconcept.com/news/index.php?page=336>>

Okay, gente. ADESSO è ora di iniziare a discutere le regole di guerra per robot autonomi. Adesso che siamo ancora in ambito teorico.

<http://www.schneier.com/blog/archives/2008/01/ethics_of_auton.html>

Un reporter è riuscito a presentare documenti legali che gli trasferiscano la proprietà dell'Empire State Building. Sì, è una bravata, ma questo genere di manovre è già stato usato per commettere frodi in passato, e continuerà a essere una tattica di frode in futuro. Il problema è che non esistono abbastanza controlli di integrità per garantire che la persona che sta "vendendo" il bene immobiliare sia davvero la persona che lo possiede.

<<http://www.foxnews.com/story/0,2933,460866,00.html>>

Monete cave -- costano poco.

<<http://www.thinkgeek.com/gadgets/tools/b308/?cpg=wnrss>>

Alcuni di voi probabilmente sanno che faccio parte del comitato consultivo dell'Electronic Privacy Information Center (EPIC). Questa organizzazione riesce a fare un gran numero di ottime cose per gli Stati Uniti e per il mondo con un budget sorprendentemente ridotto, ma qualche soldo in più non guasterebbe. Se state pensando a quali organizzazioni di beneficenza mandare un contributo questo mese, vi prego di considerare l'EPIC:

<<http://epic.org/donate/>>

<<http://www.epic.org/>>

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

Il futuro delle conversazioni effimere

Quando Barack Obama sarà presidente a tutti gli effetti dovrà abbandonare il suo BlackBerry. Ciò che preoccupa i suoi assistenti è che le sue conversazioni non ufficiali possano diventare parte della documentazione presidenziale, soggette a citazioni in tribunale e alla fine rese pubbliche come parte degli archivi storici del paese.

La realtà dell'era dell'informazione potrà anche essere particolarmente dura per il presidente, ma non è molto diversa per tutti noi. Le normali conversazioni quotidiane sono sempre state effimere. Sia di persona che per telefono, potevamo essere ragionevolmente certi che quanto detto sarebbe svanito appena uscito dalle nostre bocche. Naturalmente i boss del crimine organizzato si sono sempre preoccupati di intercettazioni telefoniche e di microfoni nascosti nelle stanze, ma quella era un'eccezione. La privacy veniva semplicemente data per scontata.

Le cose sono cambiate. Adesso conversiamo tramite email, utilizzando SMS o applicazioni di messaggia istantanea, e attraverso siti Web di social networking come Facebook, MySpace e LiveJournal. Scriviamo sui blog e usiamo Twitter. Queste conversazioni, con amici, amanti, colleghi e membri del Gabinetto, non sono per niente effimere, ma lasciano tracce elettroniche dietro di sé.

Ne siamo coscienti a livello intellettuale, ma non abbiamo ancora del tutto interiorizzato il concetto. Continuiamo a scrivere, assorbiti dalla conversazione, dimenticandoci che tutto viene registrato e che tali registrazioni potrebbero tornare a perseguirci in futuro.

Oliver North lo ha sperimentato tempo addietro, nel 1987, quando dei messaggi che credeva fossero stati cancellati vennero in realtà salvati dal sistema PROFS della Casa Bianca, e poi portati in tribunale durante il caso Iran-Contra. Bill Gates lo ha sperimentato nel 1998 quando le sue email non ufficiali vennero portate al legale della controparte come parte del processo di indagine nella causa giudiziaria antitrust contro Microsoft. Mark Foley lo ha sperimentato nel 2006 quando i suoi messaggi chat vennero registrati e resi pubblici dai minorenni con cui aveva interagito. Paris Hilton lo ha sperimentato nel 2005 quando l'account del suo cellulare fu craccato, e Sarah Palin lo ha sperimentato qualche mese fa quando il suo account email Yahoo è stato craccato. Qualcuno dell'amministrazione Bush ha capito il problema e milioni di messaggi email sono andati misteriosamente e opportunamente perduti.

La conversazione effimera sta finendo.

Il Cardinale Richelieu disse mirabilmente: "Datemi sei righe scritte dall'uomo più onesto, e ci troverò qualcosa per farlo impiccare". Quando tutte le nostre conversazioni effimere possono venire registrate per essere analizzate in un secondo momento, è necessario applicare regole diverse. La conversazione non è corrispondenza. Parole dette di fretta mentre si prende un caffè la mattina, che vengano pronunciate in una caffetteria o scritte su un BlackBerry, non sono pronunciamenti ufficiali. Le discussioni tenute durante una riunione, che abbiano avuto luogo in una sala di rappresentanza o in una chat room, non hanno lo stesso valore delle risposte date nel corso di una conferenza stampa. E la privacy non è solo legata all'aver qualcosa da nascondere: ha invece un enorme valore per la democrazia, la libertà e la nostra essenziale umanità.

Non è possibile tornare indietro: le comunicazioni elettroniche sono una realtà che è destinata a durare e anche le nostre conversazioni a voce sono in pericolo. Ma dato che la tecnologia rende le conversazioni meno effimere, occorrono delle leggi che possano fraporsi e salvaguardare la privacy. È necessaria una legge sulla privacy delle informazioni il più possibile esaustiva, che protegga le nostre informazioni e comunicazioni a prescindere da dove vengano conservate o da come vengano elaborate. Occorrono leggi che costringano le aziende a mantenerle private e a distruggerle quando non servono più. Leggi che obbligano i Provider Internet a conservare email e altre comunicazioni personali sono esattamente ciò di cui non abbiamo bisogno.

Le leggi che riguardano il governo devono essere diversi, a causa del differenziale di potere. Esporre le comunicazioni presidenziali a un successivo scrutinio pubblico aumenta le libertà perché riduce il potere del governo nei confronti delle persone. Esporre le nostre comunicazioni allo scrutinio del governo diminuisce le libertà perché riduce il nostro potere nei confronti del governo. Il presidente, così come altri membri del governo, deve poter godere di una certa libertà di intrattenersi in conversazioni effimere -- proprio come è loro permesso avere riunioni e telefonate non registrate -- tuttavia è necessario che un numero maggiore delle loro azioni sia esposto al pubblico scrutinio.

Le leggi hanno comunque i loro limiti. Legge o no, quando qualcosa viene reso pubblico è troppo tardi. E a molti di noi piace avere sottomano archivi completi della nostra corrispondenza elettronica: sono un po' come i nostri cervelli offline.

Alla fine è un fattore culturale.

L'Internet è il più grande gap generazionale dai tempi del rock and roll. Siamo ora osservando un aspetto di tale gap: la generazione più giovane chatta in via digitale, e la generazione più vecchia tratta quelle chat come fosse corrispondenza scritta. Finché i nostri CEO non terranno un blog, i nostri membri del Congresso non useranno Twitter, e i leader mondiali non si scambieranno foto dei LOLcat -- finché non avremo un'elezione presidenziale in cui entrambi i candidati avranno una cronologia completa sui siti di social networking sin da prima di essere adolescenti -- non saremo una vera e propria società dell'era dell'informazione.

Quando tutti lasceranno una traccia digitale pubblica dei loro pensieri sin dalla nascita, nessuno si farà un problema del fatto che questa traccia esista. Obama sarà anche sul 'lato giovane' del gap generazionale, ma le regole entro cui sta operando sono state scritte dal 'lato anziano'. Sarà necessaria un'altra generazione prima che cambi la tolleranza della società verso il digitalmente effimero.

Obama e il suo BlackBerry:

<<http://www.nytimes.com/2008/11/16/us/politics/16blackberry.html>>

Altre notizie sull'argomento:

<<http://abcnews.go.com/WNT/BrianRoss/story?id=2509586>>

<<http://www.washingtonpost.com/wp-dyn/content/article/2005/05/19/AR2005051900711.html>>

oppure <<http://tinyurl.com/c6hne>>

<<http://www.cnn.com/2007/POLITICS/04/13/white.house.email/index.html>>

Il valore della privacy:

<<http://www.schneier.com/essay-114.html>>

Divulgazione reciproca e potere:

<<http://www.schneier.com/essay-208.html>>

Questo articolo è originariamente apparso sul sito del Wall Street Journal.

<<http://online.wsj.com/article/SB122722381368945937.html>>

Questo articolo è un aggiornamento di un altro mio precedente scritto:

<<http://www.schneier.com/essay-109.html>>

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

Recensione di "Here Comes Everybody"

Nel 1937 Ronald Coase rispose a uno degli interrogativi più complessi in ambito economico: se i mercati sono così buoni, perché esistono le organizzazioni? Perché la gente non si mette a comprare e a vendere i propri servizi entrando direttamente in un mercato? Coase, che vinse il premio Nobel per l'economia nel 1991, rispose alla questione facendo notare i costi delle transazioni di un mercato: venditori e acquirenti devono prima trovarsi, poi raggiungere un accordo, e così via. Il teorema di Coase implica che se questi costi di transazione sono sufficientemente bassi, i mercati diretti

composti da persone hanno un senso. Ma se tali costi sono troppo elevati, è meglio che il lavoro venga svolto da un'organizzazione che assume dei dipendenti.

Da tempo gli economisti hanno compreso il concetto corollario del tetto di Coase, ossia quel punto superato il quale le organizzazioni crollano sotto il loro stesso peso -- il punto in cui assumere qualcuno, non importa quanto competente, significa maggior lavoro per tutti gli altri rispetto all'apporto che può dare il nuovo arrivato. Spesso i progetti software sbattono la testa contro il tetto di Coase: ricordo lo studio determinante di Frederick P. Brooks Jr., "The Mythical Man-Month" (Addison-Wesley, 1975), che dimostrò come aggiungere un'altra persona a un progetto possa rallentare i progressi e aumentare il numero di errori.

L'elemento di novità è quel che Clay Shirky, consulente e tecnologo sociale, chiama "Coase's Floor", il fondo di Coase, ovvero il livello al di sotto del quale troviamo progetti e attività che non valgono i loro costi organizzativi -- cose talmente esoteriche, frivole, prive di senso, o solo profondamente insignificanti che nessuna organizzazione, grande o piccola, le prenderebbe minimamente in considerazione. Cose da far scrollare il capo e pensare "Tutto questo è ridicolo".

Ricorda un po' Internet, vero? E questo è esattamente il punto di Shirky. Il suo nuovo libro, "Here Comes Everybody: The Power of Organizing Without Organizations" (Qui Vengono Tutti: Il potere di organizzare senza organizzazioni), esplora un mondo in cui i costi organizzativi sono prossimi allo zero e dove gruppi ad hoc e minimamente organizzati di non professionisti non pagati possono creare un'enciclopedia più vasta dell'Enciclopedia Britannica e un sistema operativo così sofisticato da insidiare quello di Microsoft.

Shirky insegna all'Interactive Telecommunications Program (programma interattivo di telecomunicazioni) alla New York University, ma non si tratta di un libro di stampo accademico. Privilegiando la leggibilità sul rigore, "Here Comes Everybody" è un viaggio divertente e informativo attraverso alcuni dei momenti più emblematici di Internet -- il fenomeno Howard Dean, le proteste bielorusse organizzate su LiveJournal, il cellulare perduto di una donna chiamata Ivanna, Meetup.com, i flash mob, Twitter, e altro ancora -- che Shirky utilizza per illustrare le sue argomentazioni.

Il libro è ricco di spunti profondi e all'insegna del buonsenso, che spiegano perché i giovani riescano a sfruttare meglio gli strumenti sociali, come Internet influenzi i cambiamenti sociali, e perché la maggior parte delle dissertazioni su Internet rientrino in un livello compreso fra la conversazione davanti alla cena e la pubblicazione.

Shirky fa notare che "una grandissima parte dei contenuti generati dall'utente non sono affatto 'contenuti' (nel senso di essere creati per la pubblica consultazione), o meglio sono 'contenuti' quanto una telefonata fra voi e un vostro fratello si può definire 'contenuti generati da un familiare'. La maggior parte di quel che viene creato ogni giorno è semplicemente un insieme di cose ordinarie della vita quotidiana -- pettegolezzi, piccoli aggiornamenti, pensieri ad alta voce -- ma ora viene prodotto nello stesso medium in cui si veicola il materiale prodotto professionalmente. A differenza di quest'ultimo, però, i contenuti in Internet possono essere organizzati a posteriori".

Nessuno coordina i 6-8 milioni di utenti di Flickr. Eppure su Flickr sono state pubblicate le prime foto degli attentati terroristici ai mezzi pubblici di Londra nel 2005, battendo

sul tempo i media tradizionali. Perché? Quelli che avevano cellulari con fotocamera hanno caricato le loro foto su Flickr. Si sono organizzati impiegando strumenti offerti da Flickr. Questo è il genere di organizzazione improvvisata idealmente perfetta per un mezzo come Internet. Shirky spiega come questi momenti siano precursori di un futuro che si possa organizzare autonomamente senza gerarchie formali.

Queste non-organizzazioni permettono il contributo di un insieme più esteso di persone. Un quotidiano deve pagare qualcuno che faccia delle foto e non può permettersi di assumere qualcuno che se ne stia senza far niente nella metropolitana di Londra, in attesa di qualche evento importante. Analogamente, Microsoft deve pagare un programmatore a tempo pieno, e l'Enciclopedia Britannica deve pagare chi scrive gli articoli. Ma Flickr può servirsi di una persona che possa contribuire anche con una sola foto, Linux può incanalare il lavoro di un programmatore in breve tempo, e la Wikipedia trae vantaggio anche da un apporto minimo come la correzione di un refuso. Questi aggregati di milioni di azioni che si trovavano precedentemente al di sotto del 'fondo di Coase' hanno un potenziale smisurato.

Ma un flash mob è sempre una folla. In un mondo in cui il 'fondo di Coase' è al pianterreno, spuntano le organizzazioni più varie, comprese quelle non gradite: organizzazioni politiche violente, gruppi di odio, negatori dell'Olocausto, e così via. (La trattazione di Shirky in merito ai gruppi di supporto dell'anoressia fra gli adolescenti è una lettura decisamente inquietante). Tutto questo ha conseguenze molto importanti in fatto di sicurezza, online e offline.

Non ci siamo mai resi conto di quanto la nostra sicurezza potesse attribuirsi alla distanza e alla scomodità -- a quanto sia difficile reclutare, organizzare, coordinare e comunicare senza organizzazioni formali. Quell'involontaria misura di sicurezza ora non esiste più. I malviventi, dai gruppi di hacker ai gruppi terroristici, si serviranno delle stesse tecnologie di organizzazione ad hoc che usiamo noi. E anche se si è registrato qualche successo nella chiusura di certi siti Web, gruppi di discussione e blog, queste non sono altro che misure tappabuchi.

Alla fin fine, una comunità virtuale è sempre una comunità e deve essere trattata come tale. E così come il miglior modo di proteggere un quartiere è quello di avere un poliziotto che lo pattuglia, il miglior sistema per proteggere una comunità virtuale e grazie alla presenza di una polizia virtuale.

Il crimine non è l'unico pericolo: esiste anche l'isolamento. Se le persone possono auto-segregarsi in gruppi sempre più ristretti e specializzati, allora è meno probabile che possano entrare in contatto con idee e punti di vista alternativi. Possiamo vedere una forma moderata di questo fenomeno nell'attuale tendenza politica che vede i vari partiti tutti con le proprie fonti di notizie, i propri resoconti e i propri fatti. La maggiore radicalizzazione è un altro pericolo che si cela sotto il 'fondo di Coase'.

Non si torna indietro, però. Tutti ormai abbiamo capito che Internet rende la libertà di parola un diritto molto più difficile da portar via. Come dimostra Shirky, il Web 2.0 sta avendo lo stesso effetto sulla libertà di associazione. Ci vorranno anni per vedere pienamente le conseguenze di tutto questo.

"Here Comes Everybody" condivide parte dello stesso ambito di "Wealth of Networks" di Yochai Benkler. Ma quando ho dovuto spiegare a uno dei legali della mia azienda come

Internet ha cambiato la natura della trattazione pubblica, ho consigliato il libro di Shirky.

<<http://www.amazon.com/exec/obidos/ASIN/1594201536/counterpane/>>

Il podcast di Clay Shirky:

<http://www.econtalk.org/archives/2008/10/shirky_on_coase.html>

Questo articolo è precedentemente apparso in "IEEE Spectrum".

<<http://www.spectrum.ieee.org/sep08/6631>>

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

Le news su Schneier/BT Counterpane

Schneier interverrà a una conferenza del CATO Institute conference, "Shaping the New Administration's Counterterrorism Strategy" (Definire la strategia antiterrorismo della nuova amministrazione), il 12-13 gennaio a Washington, DC.

<<http://www.cato.org/events/counterterrorism/index.html>>

Schneier ha scritto un articolo per il Guardian; è apparso anche in "The Hindu".

<<http://www.guardian.co.uk/technology/2008/nov/13/internet-passwords>>

<<http://www.hindu.com/thehindu/holnus/008200811130924.htm>>

Niente che non abbia già detto.

<<http://www.schneier.com/essay-148.html>>

L'intervista a Schneier di Datamation:

<<http://itmanagement.earthweb.com/secu/article.php/3784506/Bruce+Schneier:+Securing+Your+PC+and+Your+Privacy.htm>> oppure <<http://tinyurl.com/5at67q>>

Schneier è stato nominato una delle 25 persone più influenti nell'industria della sicurezza.

<http://www.securitymagazine.com/CDA/Articles/Cover_Story/BNP_GUID_9-5-2006_A_1000000000000484861>

oppure <<http://tinyurl.com/6fuhcv>>

Un'altra recensione di "Schneier on Security". Ricordate che è possibile ordinare copie autografate sul sito del libro. Sono ottimi regali per le feste.

<<http://www.pcpro.co.uk/reviews/241476/schneier-on-security.html>>

<<http://www.schneier.com/book-sos.html>>

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

L'FBI alimenta paure

Un'altra trama terroristica infondata.

Leggete l'articolo: "plausibile ma inconsistente", "potrebbero aver parlato di attaccare la rete metropolitana", "dettagli specifici per confermare che questo complotto sia andato al di là di una pianificazione preliminare", "l'attacco potrebbe forse essere condotto", "è plausibile, ma al momento non vi sono ancora prove che sia in procinto di essere portato avanti".

Non ho dettagli specifici, ma voglio mettere tutti in guardia: oggi potrebbe cadere dal cielo una pioggia di fuoco. I terroristi potrebbero aver discusso questo genere di tattica, probabilmente in uno dei loro incontri di pianificazione preliminare a base di tequila. Pur non essendovi ancora prove al momento che il piano sia in procinto di essere portato avanti, voglio essere molto prudente durante il periodo delle festività. Ho ho ho.

<http://www.google.com/hostednews/ap/article/ALeqM5j1NEBSpGCN1_9rZCXTwXBcnNXOxAD94MNT4O0> oppure <<http://tinyurl.com/5fhlp5>>

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

Schneier amministratore della TSA?

Su un paio di siti Web qualcuno ha suggerito che io venga nominato amministratore della TSA. Per la cronaca, non voglio quell'incarico.

Non lo voglio perché è troppo limitato. Io credo che la cosa giusta che il governo dovrebbe fare sarebbe quella di dare alla TSA molti meno soldi. Preferirei che ci proteggessero dalla minaccia generale del terrorismo invece di concentrarsi sulla minaccia più ristretta del terrorismo aereo, e preferirei che ci difendessero dalla miriade di minacce che gravano sulla nostra società invece di concentrarsi sull'unica minaccia del terrorismo. Ma il capo della TSA non può avere quelle opinioni; deve prendere il denaro che gli viene concesso e servire la funzione specifica a lui destinata. Non è granché divertente.

Ma sarei felice di fare da consulente a chiunque Obama mettesse alla guida della TSA.

Il lavoro del CTO nazionale sarebbe più interessante, ma non sono molto sicuro di volere nemmeno quello. (Avete visto il processo di selezione?)

<<http://www.foxnews.com/story/0,2933,453093,00.html>>
<http://weblog.infoworld.com/robertxcringely/archives/2008/11/the_once_and_fu.html>
> oppure <<http://tinyurl.com/6dugxe>>
<http://blogs.computerworld.com/obama_cto>

Il processo di selezione:
<<http://www.nytimes.com/2008/11/13/us/politics/13apply.html>>

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

Notizie su Skein e SHA-3

Il NIST ha pubblicato tutti i 51 candidati della prima selezione del suo concorso per la designazione di un nuovo algoritmo hash. (Gli altri contributi -- si dice che il NIST ne abbia ricevuti 64 -- sono stati scartati perché non erano completi). Lo scopo dell'Istituto è quello di pubblicare i contributi accettati entro la fine del mese, prima del Third Cryptographic Hash Workshop che si terrà in Belgio subito dopo il FSE a febbraio. I piani del NIST sono di effettuare una rapida scrematura -- per arrivare, si spera, ad averne circa una dozzina -- e poi dare alla comunità un anno circa per svolgere il lavoro di crittanalisi prima della seconda selezione nel 2010.

È possibile scaricare il pacchetto di ogni candidato dalla pagina del NIST. Lo SHA-3 Zoo è ancora la fonte migliore per ottenere informazioni di crittanalisi aggiornate. Alcune persone hanno provato a effettuare dei benchmark delle prestazioni dei vari contributi, ma naturalmente i risultati dipendono molto dall'unità di misura scelta.

Vi sono due bug nel codice di Skein. Sono oscuri ed esoterici, ma ci sono. Abbiamo revisionato sia il riferimento che il codice ottimizzato (nonché messo a disposizione nuovi vettori di prova) sul sito di Skein. Una revisione dello studio (Versione 1.1) contiene nuovi vettori di inizializzazione, nuovi vettori di prova e corregge alcuni refusi.

"Errata: La versione 1.1 dello studio, del riferimento, e del codice ottimizzato corregge un errore in cui la lunghezza della stringa di configurazione veniva passata come dimensione del blocco interno (256 bit per Skein-256, 512 bit per Skein-512 e 1024 bit per Skein-1024), invece di un valore costante di 256 bit per tutte e tre le dimensioni. Questo errore non ha alcuna importanza dal punto di vista crittografico, ma intaccava i vettori di prova e i valori di inizializzazione. Il codice revisionato inoltre sistema un bug nell'elaborazione della chiave in modalità MAC. Questo bug non ha alcun impatto sul contributo presentato al NIST".

Vi sono poi delle notizie sulle prestazioni di Skein. E due implementazioni Java. (Qualcuno vuole scrivere un'implementazione di Threefish?). In generale, il sito Web di Skein è il luogo da visitare per avere delle informazioni sempre aggiornate in merito.

Infine DarkReading ha parlato molto bene di Skein.

"Questi contributi prevedono qualche adattamento al processore Core 2. Operano in modalità 'little-endian' (una peculiarità dei processori Intel che leggono alcuni byte in ordine inverso). Permettono inoltre a un file di grosse dimensioni di essere spezzato in vari frammenti per distribuire il lavoro su più processori.

"Tuttavia, praticamente tutti i contributi presentati al concorso presentano il problema di prestazioni menzionato poco sopra. La logica che utilizzano non è destinata ad adattarsi perfettamente alle limitazioni di un processore Intel Core 2. Molti candidati avranno prestazioni ugualmente scadenti o addirittura peggiori dell'attuale algoritmo SHA-1.

"Fa eccezione Skein, creato da svariati crittografi di fama fra cui l'esperto Bruce Schneier. È stato progettato specificatamente per sfruttare tutte e tre le unità di esecuzione del Core 2 e per girare a 64 bit pieni. Ciò gli permette di avere una densità logica superiore alla concorrenza di 4-10 volte.

"È questo ciò che intendevo dire con la citazione da Matrix. Non hanno piegato il cucchiaino: hanno piegato l'algoritmo crittografico. Hanno spostato le operazioni logiche in un modo che non va a indebolire la crittografia, ma che rinforza la velocità dell'algoritmo nell'Intel Core 2.

"Nel loro studio gli autori di Skein esprimono sorpresa che una implementazione ASIC hardware personalizzata non sia più veloce dell'implementazione software. Non dovrebbero sorprendersi. Ogni volta in cui è possibile ridefinire un problema per un'esecuzione ottimale nel software, si raggiungeranno le stesse velocità che si ottengono con hardware ASIC ottimizzato. Il motivo per cui il software ha la reputazione di essere lento è perché il problema originario non viene ridefinito".

E questo è esattamente ciò che stavamo cercando di fare.

Il sito del NIST:

<<http://csrc.nist.gov/groups/ST/hash/sha-3/index.html>>
<http://csrc.nist.gov/groups/ST/hash/sha-3/Round1/submissions_rnd1.html> oppure
<<http://tinyurl.com/62532t>>
<<http://csrc.nist.gov/groups/ST/hash/timeline.html>>

SHA-3 Zoo:

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

Confronti prestazionali:

<<http://bench.cr.yp.to/ebash.html>>
<<http://eprint.iacr.org/2008/511>>
<<http://www.skein-hash.info/sha3-engineering>>

Skein:

<<http://www.skein-hash.info/>>
<<http://www.skein-hash.info/5.99-cpb>>

Skein in Java:

<<http://www.xs4all.nl/~warper/>>
<<http://www.h2database.com/skein/index.html>>

La nuova documentazione:

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

Il mio articolo sul procedimento, pubblicato da Wired:

<http://www.wired.com/politics/security/commentary/securitymatters/2008/11/securitymatters_1120> oppure <<http://tinyurl.com/5dd8nd>>

Il sito del NIST:

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

Contributi pubblici:

<http://ehash.iaik.tugraz.at/wiki/The_SHA-3_Zoo>
<[http://www.cio.com/article/461164/Amateurs and Pros Vie to Build New Crypto Standard](http://www.cio.com/article/461164/Amateurs_and_Professionals_Vie_to_Build_New_Crypto_Standard)> oppure <<http://tinyurl.com/5ntxvn>>

<http://www.darkreading.com/blog/archives/2008/11/bending_skein_c.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>>

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

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 all'indirizzo <<http://www.cryptogram.it/>>

I numeri arretrati sono disponibili su <<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) 2008 - Bruce Schneier.