

CRYPTO-GRAM
15 novembre 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:

- La funzione hash Skein
- La TSA e il sottoscritto
- News
- La crittografia quantica
- L'economia dello Spam
- Le news su Schneier/BT Counterpane
- La psicologia degli imbrogliatori
- Minaccia da trama cinematografica: i terroristi usano Twitter
- Concedere chiavi di riserva di una camera d'albergo
- P = NP?
- Commenti dei lettori

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

La funzione hash Skein

Il NIST ha inaugurato un concorso per sostituire la famiglia SHA delle funzioni hash, che ha subito attacchi sempre più frequenti.

Skein è il nostro contributo (mio e di altri sette autori: Niels Ferguson, Stefan Lucks, Doug Whiting, Mihir Bellare, Tadayoshi Kohno, Jon Callas e Jesse Walker). Quel che segue è il nostro Sommario Esecutivo:

"Skein è una nuova famiglia di funzioni hash crittografiche. Il suo design unisce velocità, sicurezza, semplicità e una notevole flessibilità, il tutto all'interno di un package modulare facile da analizzare.

"Skein è veloce. Skein-512, la nostra proposta principale, effettua l'hash dei dati a 6,1 cicli di clock per byte su una CPU a 64 bit. Ciò significa che con un processore Core 2 Duo x64 a 3,1 GHz Skein effettua l'hash dei dati a 500 MB al secondo per ciascun core -- è quindi circa due volte più veloce di SHA-512 e tre volte più veloce di SHA-256. Una modalità hash-tree velocizza ancor di più le implementazioni parallelizzabili. Skein è veloce anche con i messaggi corti: Skein-512 effettua l'hash di messaggi corti in circa 1000 cicli di clock.

"Skein è sicuro. Il suo design conservativo si basa sul block cipher Threefish. Al momento il nostro migliore attacco contro Threefish-512 è su 25 di 72 round, per un fattore di sicurezza di 2,9. Per fare un confronto, a uno stadio analogo del processo di standardizzazione, l'algoritmo di cifratura AES aveva un attacco su 6 di 10 round, per un fattore di sicurezza di 1,7 soltanto. Inoltre, Skein è dotato di una serie di proprietà probabilmente sicure, che aumentano in modo significativo la fiducia nell'algoritmo.

"Skein è semplice. Utilizzando solamente tre operazioni primitive, la funzione di compressione di Skein può essere facilmente compresa e ricordata. Il resto dell'algoritmo è una semplice iterazione di questa funzione.

"Skein è flessibile. Skein viene definito per tre dimensioni di stato interno (256 bit, 512 bit e 1024 bit), e per qualsiasi dimensione di output. Questo permette a Skein di essere un sostituto dell'intera famiglia di funzioni hash SHA molto semplice da applicare. Un sistema di argomenti espandibile e completamente opzionale rende Skein uno strumento efficace da impiegare per un gran numero di funzioni: un PRNG (generatore di numeri pseudo-casuali), uno stream cipher, una funzione di derivazione di chiavi, autenticazione senza le informazioni aggiuntive del HMAC (Hashed Message Authentication Code), e la possibilità di personalizzazione. Tutte queste funzionalità possono venire implementate con un carico di informazioni aggiuntive molto ridotto. Unitamente al large-block cipher di Threefish nel nucleo di Skein, tale design fornisce un insieme completo di primitive crittografiche simmetriche adatte alla maggior parte delle applicazioni moderne.

"Skein è efficiente su una grande varietà di piattaforme, sia hardware che software. Skein-512 può essere implementato in circa 200 byte di stato. Piccoli dispositivi, come le smart card a 8 bit, possono implementare Skein-256 utilizzando circa 100 byte di memoria. Dispositivi più grandi possono implementare le versioni maggiori di Skein per raggiungere velocità più elevate.

"Skein è stato progettato da un gruppo di esperti professionisti di crittografia, provenienti dal mondo accademico e dall'industria, con esperienza in crittografia, analisi di sicurezza, software, progettazione di chip, e implementazione di sistemi crittografici nel mondo reale. Questo ampio bacino di conoscenze ha permesso la creazione di un design equilibrato che funziona egregiamente in tutti gli ambiti di applicazione".

La scadenza fissata dal NIST era la fine di ottobre. Sembra che tutti (anche molti dilettanti) stiano lavorando a una funzione hash. Avevo previsto che il NIST ricevesse almeno 80 contributi -- ne hanno ricevuti 64. (Si confronti questo dato con i sedici

contributi ricevuti dal NIST per il concorso AES del 1998). Circa un terzo di questi contributi è di pubblico dominio al momento.

Il processo di selezione impiegherà grosso modo quattro anni. In precedenza ho definito questo genere di iniziativa un 'demolition derby' -- l'ultimo che rimane in piedi vince -- ma non è del tutto vero. Sicuramente tutti i gruppi passeranno i prossimi due anni cercando di effettuare crittanalisi reciproche, ma alla fine rimarrà un insieme di algoritmi intatti. Il NIST ne selezionerà uno basandosi sulle prestazioni e sulle funzionalità.

Il NIST ha dichiarato che l'obiettivo di questo procedimento non è scegliere lo standard migliore, ma scegliere un buon standard. Credo che sia una posizione intelligente: in questo processo, "migliore" è nemico di "buono". Il mio consiglio: ordinare immediatamente gli algoritmi basandosi su prestazioni e funzioni. Chiedere alla comunità crittografica di concentrarsi sui primi dieci-dodici della graduatoria, invece di diluire l'attenzione su tutti e 64 -- anche se mi aspetto che molti dei contributi amatoriali verranno respinti dal NIST per non essere "completi e appropriati". Altrimenti verranno bucati gli algoritmi più facili, mentre i migliori non verranno neanche analizzati.

Il sito di Skein:

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

Il codice sorgente è disponibile sul sito.

Il sito di SHA-3 (NIST):

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

I contributi per SHA-3 (27 dei quali sono di pubblico dominio):

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

Articoli di news:

<<http://www.networkworld.com/news/2008/102708-crypto-hash-algorithm-competition.html>>

oppure <<http://tinyurl.com/636snh>>

<<http://technocrat.net/d/2008/10/29/52952>>

<<http://www.techworld.com/security/news/index.cfm?newsid=106319&pagtype=all>>

oppure <<http://tinyurl.com/67odfz>>

Gli attacchi contro SHA-1:

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

Il mio liveblogging di un precedente workshop su hash del NIST:

<http://www.schneier.com/blog/archives/2005/10/nist_hash_works_1.html>

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

La TSA e il sottoscritto

The Atlantic ha pubblicato un ottimo articolo su di me che spiegavo come aggirare la sicurezza negli aeroporti. Abbiamo stampato carte d'imbarco fasulle, spiegato come

chiunque sia sulla no-fly list possa passare la sicurezza senza problemi, e abbiamo portato a bordo una quantità di liquidi superiore a quella consentita.

Kip Hawley, capo della TSA, ha risposto all'articolo sul suo blog.

Purtroppo non vi è una gran consistenza nella sua risposta. È ovvio che non vuole ammettere che abbiano controllato documenti di identità per tutto questo tempo senza scopo alcuno, pertanto si limita a emettere affermazioni generiche e vaghe, come una seppia spaventata che riempie l'acqua di inchiostro. Certo, alcune delle trovate dell'articolo sono piuttosto sciocche (a chi importa se la gente vola indossando T-shirt con scritto 'Hezbollah?'), e questo dà a Hawley l'opportunità di minimizzare le vere problematiche.

Hawley dice: "Le watch list e i controlli di identità sono misure di sicurezza importanti ed efficaci. Identifichiamo decine di individui collegati al terrorismo ogni settimana e fermiamo costantemente persone sulla No-Fly list grazie al nostro sistema di watch list".

È semplicemente impossibile che la TSA fermi decine di terroristi ogni settimana. Se ciò fosse vero, l'amministrazione continuerebbe a strombazzarlo in lungo e in largo -- sarebbe un'incredibile storia di successo nella sua guerra al terrorismo. Ma se ci fate caso, Hawley non dice esattamente questo: li chiama "individui collegati al terrorismo". E che caspita significa, esattamente? Persone talmente pericolose da non poter avere il permesso di volare in alcun modo, eppure così innocenti che non si possono arrestare, nemmeno in virtù dei provvedimenti del Patriot Act.

E se il segretario Chertoff dice il vero quando afferma che vi sono soltanto 2.500 persone sulla no-fly list e meno di 16.000 persone sulla lista dei 'selezionati' (individui che devono essere sottoposti a ulteriori controlli), e che la maggior parte di esse vive fuori dagli Stati Uniti, allora è semplicemente impossibile che la TSA identifichi "decine" di queste persone ogni settimana. I conti, banalmente, non tornano.

E non credo nemmeno a questa affermazione: "L'analisi comportamentale funziona e oggi abbiamo 2.000 agenti addestrati negli aeroporti. Ci avvertono quando individuano persone che possano rappresentare una minaccia, ma che possono anche avere con sé oggetti che sfuggono ad altri livelli di sicurezza".

Per funzionare funziona, ma non mi sembra che la TSA lo stia facendo in maniera appropriata. (Se volete vedere come viene effettuato correttamente, volate con El Al). Ma qui credo che Hawley stia facendo un po' di manipolazione psicologica. Come per gli sky marshal, il vero vantaggio dell'analisi comportamentale non sta nell'applicarla o meno, ma nel fatto che i criminali CREDANO che venga applicata. Se credono che stiate effettuando analisi comportamentale ai checkpoint di sicurezza, o che avete disposto degli sky marshal su ogni aereo, allora non è necessario che lo facciate per davvero. Il deterrente è la minaccia, non il sistema di sicurezza vero e proprio.

Non mi sorprende nemmeno quanto segue: "Oggetti che le persone si portano indosso -- che siano una 'beer belly' (ossia la 'pancia da birra', una sorta di tasca da portare in vita per nascondere birra o altri oggetti) oppure oggetti nascosti in zone molto private, sono il motivo principale per cui nei prossimi mesi andremo acquistando più di 100 scanner del corpo intero e col tempo ne implementeremo un numero sempre maggiore.

Nel frattempo utilizziamo dispositivi manuali che rilevano il perossido di idrogeno e altri composti esplosivi, e perquisizioni che richiedono uno screening privato".

Le misure di sicurezza opzionali non funzionano perché i criminali non faranno altro che evitare di ricorrere a quelle strategie. È lo stesso caso di quelle macchine air-puff presenti ultimamente in alcuni aeroporti. Con ogni probabilità sono ottime per rilevare residui di esplosivo sui vestiti, ma tutte le volte che ho visto queste macchine in azione, i passeggeri hanno avuto la possibilità di scegliere se passare dalla corsia dove erano disposte oppure di cambiare corsia evitando il controllo. Quali benefici può offrire un simile sistema?

Di tutto quel che ha detto Hawley, ciò che più si avvicina a una vera risposta è che i terroristi potrebbero essere presi mentre rubano carte di credito. "Utilizzare carte di credito rubate e documenti falsi come metodo per aggirare le watch list è la prova che spingere i terroristi a servirsi di tattiche sempre più rischiose abbia un certo valore dal punto di vista della sicurezza".

Su questo ha ragione. E, a dirla tutta, si trattò della mia risposta più farraginosa durante l'intervista originale. Pensandoci in un secondo momento, è molto più probabile che a comprare i vari biglietti aerei sia una persona con la fedina penale pulita e una carta di credito legittima.

Questa è una novità: "Stiamo collaudando degli scanner delle carte d'imbarco e una protezione crittografica in otto aeroporti per il momento, ma col tempo verranno implementati in un numero maggiore di aeroporti".

Se ignoriamo per un momento quella sciocchezza degli "otto aeroporti" (a meno di non utilizzare gli scanner in tutti gli aeroporti, i criminali sceglieranno un aeroporto privo di questa misura di sicurezza per sferrare il loro attacco), si tratta di un'ottima idea. Il motivo per cui il mio attacco funziona, la ragione per cui mi è possibile passare il checkpoint della TSA con una carta d'imbarco fasulla, è che la TSA non verifica mai che le informazioni sulla carta d'imbarco corrispondano a una prenotazione legittima. Se tutti i checkpoint della TSA avessero degli scanner di carte d'imbarco che si collegassero ai computer delle linee aeree, questo attacco non funzionerebbe. (La cosa interessante è che ho notato proprio questo sistema in vigore all'aeroporto di Dublino il mese scorso).

E per finire: "Fermare il terrorista 'James Bond' è davvero un lavoro di squadra e sono assolutamente d'accordo che il metodo migliore per bloccare quel tipo di attacchi sia uno sforzo congiunto di intelligence e forze dell'ordine".

La questione non è "Fermare il terrorista 'James Bond'", ma fermare il terrorismo. E se tutto questo lavoro concentrato sugli aeroporti, anche nel caso in cui inizi a funzionare davvero, non farà altro che spingere i terroristi verso altri obiettivi, allora non avremo ottenuto una sicurezza granché efficace con il nostro denaro.

Articolo dell'Atlantic:

<<http://www.theatlantic.com/doc/200811/airport-security>>

Risposta di Hawley:

<<http://www.tsa.gov/blog/2008/10/tsas-take-on-atlantic-article.html>>

Chertoff sulla no-fly list:

<<http://www.cnn.com/2008/TRAVEL/10/22/no.fly.lists/index.html>>

Hawley risponde ai miei commenti sul mio blog. Sì, è proprio lui.

<http://www.schneier.com/blog/archives/2008/10/kip_hawley_resp.html#c321445>

oppure <<http://tinyurl.com/6692n5>>

La mia intervista con Hawley dello scorso anno:

<<http://www.schneier.com/interview-hawley.html>>

Fra le altre cose, Kip Hawley afferma che la TSA potrebbe diventare più permissiva per quanto riguarda le restrizioni sulle quantità di liquidi ammessi. I passeggeri dovranno sempre toglierli dal bagaglio, ma potranno essere più grandi di 88 ml. Il motivo, così dice Hawley, è che le tecnologie di rilevamento stanno migliorando, non che la minaccia sia minore.

<<http://www.tsa.gov/blog/2008/10/path-forward-on-liquids.html>>

Sono scettico, ovviamente, ma leggete il suo post: è interessante.

L'Atlantic ha lanciato un concorso, basato sul commento di Hawley per cui la TSA sarebbe sostanzialmente dedita alla cattura di terroristi stupidi: "E quindi ecco il concorso: Come si potrebbe applicare il Principio di Hawley della Mediocrità Federale ad altre operazioni governative?"

<http://jeffreygoldberg.theatlantic.com/archives/2008/10/new_contest_can_you_outla_me_th.php>

oppure <<http://tinyurl.com/6e5t7w>>

Non è come il mio concorso Minaccia da Trama Cinematografica, ma è ugualmente divertente.

E infine, che farebbe la TSA con questo?

<<http://www.boingboing.net/2008/10/24/chanel-gun-heel.html>>

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

News

Dalla Conferenza LEET '08: "Designing and implementing malicious hardware" (Progettare e implementare hardware maligno) di Samuel T. King, Joseph Tucek, Anthony Cozzie, Chris Grier, Weihang Jiang e Yuanyuan Zhou.

<http://www.usenix.org/event/leet08/tech/full_papers/king/king.pdf>

Abbigliamento a prova di taser:

<<http://technology.newscientist.com/article/mg19626296.400>>

Un poster di avviso: "In Case of Terrorist Attack, Do Not Discard Brain" (In caso di attacco terroristico, non buttate via il cervello)

<<http://miscellanea.wellingtongrey.net/2008/10/12/warning-in-case-of-terrorist-attack-do-not-discard-brain/>>

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

Malgrado sia fortemente contrario a un documento di identità nazionale, ho costantemente sostenuto che sia una buona idea concedere delle tessere di identità munite di sicurezza forte a gruppi di lavoratori come i portuali.

<http://www.boston.com/news/local/massachusetts/articles/2008/10/06/high_tech_id_cards_rolling_out_at_ports/?rss_id=Boston.com+--+Massachusetts+news>

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

La mia posizione sui documenti di identità nazionale:

<<http://www.schneier.com/testimony-realid.html>>

Nella British Columbia del nord sono avvenute due esplosioni in due oleodotti. Questo estratto mi conforta: "Gli investigatori stanno trattando le esplosioni come atti di vandalismo, non di terrorismo, ha dichiarato Shields. 'Secondo il codice penale andrebbe caratterizzato come danno, atto illecito, che è vandalismo intenzionale. Non vogliamo definirlo terrorismo. Si tratta di luoghi molto isolati e non sembra vi sia stata l'intenzione di far del male a persone', ha detto".

<<http://www.cbc.ca/canada/british-columbia/story/2008/10/16/bc-second-pipeline-explosion-dawson-creek.html>>

oppure <<http://tinyurl.com/6dk6zm>>

Al contrario, a Philadelphia, il progetto di un treno della metropolitana è stato criticato perché le persone possono guardar fuori anche dalla parte frontale. E... ehm... anche i terroristi potranno guardar fuori dalla parte frontale, e tutti sappiamo quanto siano pericolosi i terroristi.

<http://www.philly.com/inquirer/local/pa/chester/20081017_SEPTA_engineers_dislike_new_cars_cabs.html>

oppure <<http://tinyurl.com/6hy5h7>>

Pare che gli ingegneri abbiano altri piani -- le cabine dei nuovi treni sono troppo piccole -- e stiano usando la sicurezza solo come scusa:

<<http://septawatch.blogspot.com/2008/10/septa-engineers-dont-want-new.html>>

oppure <<http://tinyurl.com/5ef8tc>>

E nel Regno Unito continua a esserci un forte allarmismo terroristico:

<http://news.bbc.co.uk/1/hi/uk_politics/7674775.stm>

Una storia allarmistica che parla di terroristi che celano le loro comunicazioni in immagini pedopornografiche.

<<http://www.telegraph.co.uk/news/uknews/3215115/Terrorists-use-child-porn-to-exchange-information.html>>

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

<<http://www.timesonline.co.uk/tol/news/uk/crime/article4959002.ece>>

<<http://www.foxnews.com/story/0,2933,439641,00.html>>

Terroristi e sconosciuti che prendono di mira i nostri bambini sono due delle cose che instillano più paura nelle persone. Mettetele insieme, e non vi è limite ai tipi di legge che riuscirete a far approvare. Un commento sul mio blog: "Perché i terroristi dovrebbero nascondere messaggi incriminanti dentro fotografie incriminanti? Sarebbe come se i contrabbandieri di droga nascondessero chili di cocaina in balle di marijuana".

<http://www.schneier.com/blog/archives/2008/10/terrorists_and_2.html#c319818>

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

Intercettare quanto viene battuto su una tastiera, a una decina di metri di distanza, in un'altra stanza.

<http://www.theregister.co.uk/2008/10/20/keyboard_sniffing_attack/>

<<http://news.bbc.co.uk/2/hi/technology/7681534.stm>>
<<http://lasecwww.epfl.ch/keyboard/>>

ANSI Cyberrisk Calculation Guide (Guida per calcolare i rischi di sicurezza cibernetica pubblicata dall'ANSI)

<<http://www.darkreading.com/security/perimeter/showArticle.jhtml?articleID=211600785>>

oppure <<http://tinyurl.com/5enqj6>>

<<http://webstore.ansi.org/cybersecurity.aspx>>

In genere evito di parlare di politica elettorale (Crypto-Gram tratta di altri argomenti) ma val la pena discutere questo commento di Barack Obama sulla sicurezza e i compromessi:

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

I crittografi hanno scherzato a lungo sulla cosiddetta 'rubber-hose cryptanalysis', ossia estorcere a qualcuno le chiavi con la forza. Beh, pare che una cosa del genere sia successa davvero in Turchia:

<http://news.cnet.com/8301-13739_3-10069776-46.html>

Storia agghiacciante di un detenuto nel braccio della morte in possesso illecito di un cellulare.

<<http://www.statesman.com/news/content/news/stories/local/10/21/1021deathrow.html>>

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

Se non riusciamo a tener fuori le merci di contrabbando dalle prigioni, come possiamo sperare di tenerle lontano dagli aerei?

Questa è una storia che illustra come le persone intelligenti possano essere neutralizzate mediante stupide procedure.

<<http://consumerist.com/5069018/how-outsourced-call-centers-are-costing-millions-in-identity-theft>>

oppure <<http://tinyurl.com/59p6ww>>

Scambiare i codici a barre dei prodotti per comprare merce a un prezzo più basso non è certo nuova come truffa, ma come è possibile riuscire a ottenere merci per un valore complessivo di più di un milione di dollari con questa truffa? Ci vuole un gran numero di commessi veramente incapaci.

<<http://www.daytondailynews.com/n/content/oh/story/news/local/2008/10/24/ddn102408tidwellweb.html?imw=Y>>

oppure <<http://tinyurl.com/696xy7>>

Video di una conferenza sugli hack dei codici a barre:

<<http://video.google.com/videoplay?docid=-5716320056489246991&hl=en>>

Proteggere l'America dal terrorismo controllando le webcam delle distillerie: una storia bizzarra che si è rivelata piuttosto banale.

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

"A Look at Terrorist Behavior: How They Prepare, Where They Strike" (Osservando il comportamento dei terroristi: come si preparano, dove colpiscono), di Brent Smith, National Institute of Justice Journal, N. 260, 2008.

<<http://www.ncjrs.gov/pdffiles1/nij/222900.pdf>>

"How Terrorist Groups End: Lessons for Countering al Qa'ida" (Come finiscono i gruppi terroristici: lezioni per contrastare al Qa'ida), di Seth G. Jones e Martin C. Libicki, RAND Corporation, 2008.

<http://www.rand.org/pubs/monographs/2008/RAND_MG741-1.pdf>

Duplicare le chiavi dalle fotografie:

<<http://www.physorg.com/news144519246.html>>

<http://vision.ucsd.edu/~blaxton/pagePapers/laxton_wang_savage_ccs2008.pdf>

oppure <<http://tinyurl.com/5nvru9>>

Un tribunale statunitense ha stabilito che effettuare hashing equivale a effettuare una perquisizione. Un'ordinanza ottima e interessante.

<http://www.schneier.com/blog/archives/2008/11/us_court_rules.html>

L'India ha sperimentato una conseguenza negativa del divieto di condurre ricerche di sicurezza. Dei terroristi sono riusciti a trovare il modo di clonare le SIM card dei cellulari. I 'buoni' non sapevano che fosse possibile, perché non possono condurre ricerche in merito: "Gli esperti hanno affermato che nessuno ha compiuto alcuna ricerca sulla clonazione delle SIM card perché tale attività è vietata in questo paese".

<<http://timesofindia.indiatimes.com/PDATOI/pdaarticleshow/3670337.cms>>

Se i 'buoni' non possono neanche partecipare, i 'cattivi' l'avranno sempre vinta.

Un sempre maggiore allargamento delle competenze delle leggi antiterrorismo nel Regno Unito. Si sfruttano le leggi per fermare i cittadini che portano fuori i bidoni della spazzatura nel giorno sbagliato.

<<http://scotlandonsunday.scotsman.com/scotland/Town-halls-resort-to-spy.3906463.jp>>

oppure <<http://tinyurl.com/64wmh2>>

<<http://www.dailymail.co.uk/news/article-1082225/March-dustbin-Stasi-Half-councils-use-anti-terror-laws-watch-people-putting-rubbish-wrong-day.html?ITO=1490>>

oppure <<http://tinyurl.com/5aw4qq>>

Aspidistra, l'affascinante vicenda di un attacco radio man-in-the-middle della Seconda Guerra Mondiale.

<[http://en.wikipedia.org/wiki/Aspidistra_\(transmitter\)](http://en.wikipedia.org/wiki/Aspidistra_(transmitter))>

<<http://www.schneier.com/blog/archives/2008/11/aspidistra.html>>

Craccato il protocollo WPA:

<<http://arstechnica.com/articles/paedia/wpa-cracked.ars/1>>

<<http://dl.aircrack-ng.org/breakingwepandwpa.pdf>>

<<http://isc.sans.org/diary.html?storyid=5300&rss>>

<<http://gizmodo.com/5078317/wpa-wi+fi-security-gets-cracked-your-network-is-no-longer-secure>>

oppure <<http://tinyurl.com/5qc26g>>

<<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9119258>>

oppure <<http://tinyurl.com/56rzgr>>

<<http://www.heise-online.co.uk/news/WPA-alleged-to-be-crackable-in-less-than-15-minutes--/111906>>

oppure <<http://tinyurl.com/6o63ko>>

La censura a Dubai è trasparente, e comprende un processo di appello:
<http://www.schneier.com/blog/archives/2008/11/censorship_in_d.html>

Leggere una lettera partendo dalla busta in cui si trovava:
<<http://www.physorg.com/news145517878.html>>

Utilizzare la funzione di aggiornamento incrementale dei file PDF per osservare l'autore di un malware mentre crea il suo exploit:
<<http://blog.didierstevens.com/2008/11/10/shoulder-surfing-a-malicious-pdf-author/>>
oppure <<http://tinyurl.com/684s8t>>

Ridurre il rischio dell'estinzione umana:
<http://www.upmc-biosecurity.org/website/resources/publications/2007_orig-articles/2007-10-15-reducingrisk.html>
oppure <<http://tinyurl.com/675nkm>>

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

La crittografia quantica

La crittografia quantica torna a far parlare di sé, e l'idea di fondo è ancora straordinariamente affascinante, in teoria, e quasi totalmente inutile nella realtà.

L'idea alla base della crittografia quantica è che due persone che comunicassero attraverso un canale quantico potrebbero avere la certezza assoluta che nessuno le sta ascoltando. Secondo il principio di indeterminazione di Heisenberg, chiunque misuri un sistema quantico deve necessariamente disturbarlo, e tale disturbo avverte gli utenti legittimi della presenza dell'intercettatore. Nessuna interferenza, nessuna intercettazione, punto.

Questo mese si sono viste notizie su una nuova rete di distribuzione di chiavi quantiche a Vienna, e una nuova tecnica di distribuzione di chiavi quantiche proveniente dalla Gran Bretagna. È tutto davvero fantastico, ma titoli come quello della BBC, "Lanciata una crittografia 'impenetrabile'", mi sembrano un po' eccessivi.

Le nozioni scientifiche alle fondamenta della crittografia quantica sono state sviluppate, insieme a dei prototipi, nei primi anni Ottanta da Charles Bennett e Giles Brassard, e da allora sono stati compiuti continui passi avanti da un punto di vista ingegneristico. Ne descrivo il sostanziale funzionamento in Applied Cryptography, Seconda Edizione (pagg. 554-557). Esiste almeno una azienda che vende prodotti per la distribuzione di chiavi quantiche.

Si noti che tutto questo è completamente distinto dal calcolo quantistico, il quale anch'esso ha delle conseguenze in ambito crittografico. Molti gruppi stanno lavorando alla progettazione e costruzione di un computer quantico, che è profondamente diverso da un computer tradizionale. Se ne venisse costruito uno -- e qui stiamo parlando di fantascienza -- esso potrebbe fattorizzare i numeri e risolvere problemi di logaritmi discreti assai rapidamente. In altre parole, potrebbe compromettere tutti gli algoritmi a chiave pubblica usati più comunemente oggi. Per la crittografia simmetrica la situazione

non è così disperata: un computer quantico sarebbe in grado di dimezzare la lunghezza delle chiavi, per cui una chiave a 256 bit sarebbe sicura soltanto come una chiave a 128 bit odierna. Un panorama piuttosto grave, ma distante anni da una sua realizzazione pratica. Credo che il computer quantico migliore oggi disponibile possa fattorizzare il numero 15.

Se da un lato apprezzo molto la scienza legata alla crittografia quantica (sono laureato in fisica), dall'altro non ne vedo alcun valore commerciale. Non credo risolva nessun problema di sicurezza che necessiti di risoluzione. Non credo che valga la pena pagare per questa crittografia, e non riesco a immaginare nessuno che voglia acquistarla e implementarla, a parte qualche tecnofilo. I sistemi che ne fanno uso non diventano magicamente impenetrabili, perché la componente quantica non risolve i punti deboli del sistema.

La sicurezza è una catena, ed è forte tanto quanto il suo anello più debole. La crittografia matematica, malgrado a volte sia pessima, è l'anello più forte nella maggioranza delle catene di sicurezza. I nostri algoritmi a chiave simmetrica e pubblica sono molto buoni, anche se non si basano su una teoria matematica granché rigorosa. I veri problemi sono altrove: sicurezza informatica, sicurezza di rete, interfaccia utente, e così via.

La crittografia è un'area della sicurezza che possiamo coltivare bene. Già abbiamo buoni algoritmi di criptatura, buoni algoritmi di autenticazione e buoni protocolli di accordo sulle chiavi. Forse la crittografia quantica può irrobustire quell'anello, ma perché dovrebbe importare a qualcuno? Esistono problemi di sicurezza molto più importanti di cui preoccuparsi, ed è più sensato concentrare gli sforzi su di essi.

Come ho affermato più volte, è come difendersi da un aggressore in avvicinamento conficcando un grosso palo nel terreno. È inutile discutere se il palo debba essere alto 25 metri o 50 metri, perché tanto l'aggressore lo eviterà. Anche la crittografia quantica non "risolve" ogni cosa della crittografia: le chiavi vengono scambiate con i fotoni, ma la parte della criptatura vera e propria è lasciata ad un normale algoritmo matematico.

Sono sempre a favore della ricerca nel campo della sicurezza, e mi ha interessato seguire gli sviluppi della crittografia quantica. Ma come prodotto, non ha futuro. Non è che la crittografia quantica possa risultare insicura; è che la crittografia tradizionale è già sufficientemente sicura.

News:

<<http://news.bbc.co.uk/2/hi/science/nature/7661311.stm>>

<http://news.cnet.com/8301-1009_3-10064219-83.html?part=rss&subj=news&tag=2547-1_3-0-5>

oppure <<http://tinyurl.com/4bzipwb>>

<http://www.theregister.co.uk/2008/10/09/quantum_crypto_turbo_charged/>

Bibliografia sulla crittografia quantica:

<<http://www.cs.mcgill.ca/~crepeau/CRYPTO/Biblio-QC.html>>

Commercializzazione:

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

Il calcolo quantistico:

<http://en.wikipedia.org/wiki/Quantum_computer>

Ulteriori commenti sui recenti articoli in proposito:

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

Questo articolo è originariamente apparso su Wired.com.

<http://www.wired.com/politics/security/commentary/securitymatters/2008/10/securitymatters_1016>

oppure <<http://tinyurl.com/4beb94>>

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

L'economia dello Spam

I ricercatori si sono infiltrati nel worm Storm e ne hanno monitorato l'attività.

"Dopo 26 giorni e circa 350 milioni di messaggi email, le vendite risultanti sono state soltanto 28 -- per un tasso di conversione di molto inferiore allo 0,00001%. Di queste vendite, tutte tranne una riguardavano prodotti di aumento delle prestazioni maschili e il prezzo medio è stato di circa 100 dollari. Prese insieme, queste conversioni avrebbero portato profitti per 2.731,88 dollari -- poco più di 100 dollari al giorno per il periodo di osservazione, o 140 dollari al giorno nei periodi in cui la campagna era attiva. Tuttavia il nostro studio si è interposto soltanto in una piccola frazione della rete globale di Storm -- diciamo all'incirca l'1,5%, basandoci sulla frazione di worker bot di cui abbiamo effettuato il proxy. Pertanto, i profitti totali giornalieri attribuibili alla campagna farmaceutica di Storm sono più probabilmente vicini ai 7.000 dollari (o a 9.500 dollari nei periodi di attività della campagna). Secondo una logica analoga, stimiamo che le campagne auto-generate da Storm possano produrre tra i 3.500 e gli 8.500 nuovi bot al giorno.

"Mantenendo il presupposto che i dati da noi raccolti siano rappresentativi nel tempo (un presupposto, lo riconosciamo, piuttosto pericoloso quando si ha a che fare con campioni così piccoli), possiamo estrapolare che, se venisse propagato continuamente e costantemente, lo spam farmaceutico generato da Storm produrrebbe circa 3,5 milioni di dollari di profitti in un anno. Questa cifra potrebbe essere ancora più elevata se le farmacie pubblicizzate attraverso lo spam dovessero sperimentare un utilizzo continuativo del servizio. Un po' meno di 'milioni di dollari al giorno', ma sicuramente si tratta di un giro d'affari assai florido".

Naturalmente gli autori fanno notare che è pericoloso lasciarsi andare a questo tipo di generalizzazioni: "Siamo i primi ad ammettere che questi risultati rappresentano un solo punto di accesso ai dati e non sono necessariamente indicativi dello spam nel suo insieme. Campagne differenti, che fanno uso di tattiche diverse per commercializzare prodotti diversi, produrranno senza dubbio anche dei risultati diversi. Sconsigliamo caldamente ad altri ricercatori di servirsi dei tassi di conversione da noi rilevati in queste campagne basate su Storm per giustificare presupposti in qualunque altro contesto".

Lo spam è completamente basato sull'economia. Se inviare posta indesiderata costa un dollaro fra carta, affitto degli elenchi di nominativi e spese postali, un promotore commerciale ha bisogno di un tasso di conversione ragionevole affinché la campagna valga la spesa. Se inviare posta indesiderata non costa praticamente nulla, diventa accettabile anche un tasso di conversione di uno in un milione.

<<http://www.icsi.berkeley.edu/pubs/networking/2008-ccs-spamalytics.pdf>>
<http://voices.washingtonpost.com/securityfix/2008/11/study_spam_still_profitable_at.html>
oppure <<http://tinyurl.com/5flska>>
<http://www.theregister.co.uk/2008/11/10/storm_botnet_spam_economics/>

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

Le news su Schneier/BT Counterpane

Una recensione del libro "Schneier on Security":
<<http://books.slashdot.org/article.pl?sid=08/10/20/1344203>>

L'intervista a Schneier del Dr. Dobb's Journal.
<<http://www.ddj.com/security/210605067>>
Molto prima della prima edizione di Applied Cryptography, il Dr. Dobb's Journal pubblicò i miei primi scritti sulla crittografia.

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>>

L'audio dell'intervista sul mio intervento alla RSA Conference di Londra il mese scorso:
<https://365.rsaconference.com/blogs/podcast_series_rsa_conference_europe_2008/2008/10/26/session-preview-with-bruce-schneier>
oppure <<http://tinyurl.com/5faqps>>

Un mio articolo sulla scelta di buone password è apparso sul Guardian.
<<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 in precedenza.

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

La psicologia degli imbrogliatori

Un'ottima storia: "Il mio imbroglio (a breve termine) preferito in assoluto fa guadagnare al truffatore solo pochi dollari per volta, ma mi piace tantissimo. Questi tizi avevano l'abitudine di presentarsi porta a porta negli anni Settanta vendendo lampadine, e si offrivano di sostituire personalmente ogni singola lampadina in casa vostra, in modo che tutte le vostre vecchie lampadine sarebbero state sostituite con

lampadine nuove, e vi sarebbe costato, diciamo, 5 dollari -- quindi una frazione di quanto vi sarebbe costato acquistare una serie di lampadine nuove. Il tizio si presenta, cambia ogni lampadina, tutte le lampadine presenti in casa, e lo fa davvero, potete controllare, e tutte funzionano a meraviglia. Poi raccoglie tutte le vostre lampadine che ha cambiato, va alla porta accanto e le vende al vicino. Quindi in realtà sta semplicemente spostando le lampadine da una casa all'altra e facendo pagare alla gente una piccola somma di denaro per fare il lavoro".

<<http://www.abc.net.au/rn/lawreport/stories/2008/2376933.htm>>

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

Minaccia da trama cinematografica: i terroristi usano Twitter

L'idea che sia in qualche modo preoccupante che i terroristi possano utilizzare Twitter è ridicola. Naturalmente i criminali si serviranno di tutti i mezzi di comunicazione disponibili al resto della società. Devono comunicare fra loro, dopotutto. Useranno anche automobili, rubinetti e ristoranti self-service. E con ciò?

Questo commento centra perfettamente la questione: "Steven Aftergood, un analista di intelligence di lungo corso alla Federation of the American Scientists, non ha rigettato quanto presentato dall'Esercito senza pensarci. Ma non crede nemmeno che si abbia a che fare con una minaccia terribilmente grave. 'Le esercitazioni di red teaming per anticipare le operazioni dell'avversario sono fondamentali. Ma è necessario che siano ispirate da un senso di ciò che è realistico e importante e di ciò che non lo è', ha dichiarato a Danger Room. 'Se abbiamo il tempo di preoccuparci delle 'minacce di Twitter' allora siamo in forma. Voglio dire, è importante mantenere un certo senso delle proporzioni'".

<<http://www.computerweekly.com/Articles/2008/10/28/232944/terrorists-could-use-twitter-for-attacks-says-us-intelligence.htm>>

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

<<http://www.fas.org/irp/eprint/mobile.pdf>>

<<http://www.fas.org/blog/secretcy/2008/10/twitter.html>>

<<http://blog.wired.com/defense/2008/10/terrorist-cell.html>>

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

Concedere chiavi di riserva di una camera d'albergo

È un compromesso di sicurezza difficile. Gli ospiti dell'albergo perdono le chiavi della loro stanza, e il personale dell'hotel deve essere accomodante. Ma al tempo stesso non può concedere chiavi a tutti coloro che affermano di averle perdute. Solitamente, negli alberghi viene richiesto un documento di identità prima di concedere una chiave di riserva e, se l'ospite non ha con sé il portafoglio, mandano su qualcuno con la chiave a controllare i documenti.

Normalmente è un sistema che funziona bene, ma è in corso una causa legale a Brisbane, dove pare che un albergo abbia dato la chiave a qualcuno che ha poi molestato sessualmente la donna che aveva affittato la camera. "Nella causa civile iniziata ieri, la donna sostiene che l'individuo abbia ottenuto la chiave di riserva della sua stanza da un membro del personale dell'albergo".

L'articolo non dice che tipo di autenticazione l'albergo abbia richiesto o ricevuto.

<<http://www.brisbanetimes.com.au/news/queensland/room-key-given-to-rapist-hotel-guest/2008/10/29/1224956099579.html>>
oppure <<http://tinyurl.com/6gkzda>>

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

P = NP?

Varie persone mi hanno inviato uno studio che "prova" che $P \neq NP$. Questo genere di studi appare regolarmente, e il mio consiglio è di non prestare attenzione a nessuno di essi. G.J. mantiene un elenco di questi studi -- ne ha raccolti 43 finora -- e fa notare che: "I seguenti paragrafi presentano un elenco di molti studi che cercano di contribuire alla questione P-versus-NP. Fra tutti questi studi, soltanto uno è precedentemente apparso in una pubblicazione sottoposta a peer review, è stato verificato accuratamente dagli esperti del campo, e la sua correttezza è accettata dalla comunità di ricerca: lo studio di Mihalis Yannakakis. (E questo studio non risolve la diatriba del P-versus-NP, ma illustra 'soltanto' che un determinato approccio per risolvere definitivamente tale diatriba non funzionerà mai)".

Naturalmente, dato che esiste un premio di un milione di dollari per risolvere la questione, aspettatevi di veder proliferare tutti questi 'studi'.

Lo studio più recente:

<<http://arxiv.org/abs/0810.5056>>

L'elenco di Woeginger:

<<http://www.win.tue.nl/~gwoegi/P-versus-NP.htm>>

Il Millennium Prize:

<<http://www.claymath.org/millennium/>>

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

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 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) 2008 - Bruce Schneier.