

CRYPTO-GRAM
15 maggio 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:

- Felice Decimo Anniversario
- Tecnologie a duplice uso e la questione di equità
- Attraversare le frontiere con computer portatili e PDA
- News
- Il vincitore del Terzo Concorso "Minaccia da Trama Cinematografica"
- La RSA Conference
- Preferenze di rischio negli scimpanzé e nei bonobo
- Le news su Schneier/BT Counterpane
- Il Canile: Passwordsafe.com
- L'etica della ricerca delle vulnerabilità
- I nostri dati, noi stessi
- Commenti dei lettori

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

Felice Decimo Anniversario

Dieci anni fa ho iniziato a scrivere Crypto-Gram. Era una newsletter mensile scritta interamente da me. Nessuna rubrica scritta da autori ospiti. Niente pubblicità. Soltanto io che scrivevo di sicurezza e pubblicavo Crypto-Gram il 15 di ogni mese, tutti i mesi. Ora, dopo 120 numeri, nulla di tutto questo è cambiato.

Ho dato il via a Crypto-Gram perché sentivo di aver molto da dire in merito alla sicurezza, e scrivere commenti chilometrici era un'operazione troppo lenta e saltuaria. Certo, di tanto in tanto scappava l'articolo occasionale sulla rivista di turno, ma anche quei contributi erano troppo lenti e saltuari. Crypto-Gram doveva essere il mio punto di vista personale sulla sicurezza, inviata direttamente a chi volesse leggerla.

Inizialmente avevo pensato di rendere Crypto-Gram una pubblicazione a pagamento. Conoscevo varie newsletter che si finanziavano attraverso quote di iscrizione, e ho pensato che con duecento iscritti che pagassero ognuno 150 dollari circa, Crypto-Gram si sarebbe sostenuta molto bene. Non ricordo perché cambiai idea (forse qualcuno mi convinse a farlo, forse ci arrivai da solo), ma è stata in assoluto la migliore decisione che io abbia preso nei confronti di questa newsletter. Se avessi chiesto denaro, nessuno l'avrebbe letta. Essendo gratis, gli iscritti furono moltissimi.

Alla fine del primo giorno di pubblicazione gli iscritti erano 457. Dopodiché, la circolazione si diffuse lentamente ma costantemente. Ecco i totali relativi al mese di maggio di ogni anno:

1999	15.964
2000	33.827
2001	45.832
2002	58.046
2003	66.368
2004	75.907
2005	83.835
2006	87.839
2007	92.488
2008	98.618

Questi numeri nascondono molti altri lettori, come le decine di migliaia che oggi leggono Crypto-Gram sul Web. Conosco inoltre persone che inoltrano la newsletter a centinaia d'altre. Esistono svariate edizioni tradotte in altre lingue che hanno le loro quote di iscritti. In questo periodo stimo di avere circa 25.000 lettori non inclusi in quelle cifre.

Non ho idea da dove venne il primo gruppo di iscritti, né ricordo come faceva la gente a iscriversi prima che fosse pronto il form sulla pagina Web. Ricordo però la prima grande impennata di iscritti: fu dopo il mio numero speciale a seguito dell'11 settembre 2001. Scrisi qualcosa di breve per il numero di settembre, ma presto mi resi conto che non potevo smettere. Due settimane dopo pubblicai un numero speciale sugli attacchi terroristici. I lettori inoltrarono quel numero a più riprese, e il risultato furono molti nuovi iscritti.

I commenti dei lettori iniziarono prima, nel dicembre 1998. Stavano arrivando commenti davvero intelligenti da parte dei miei lettori, soprattutto da parte di chi non era d'accordo con me, e volli pubblicarne alcuni. Certe differenze di vedute erano piuttosto estreme. Nell'ottobre 1998 inaugurai una rubrica chiamata "Il Canile", in cui mi prendevo gioco di prodotti di sicurezza truffaldini commercializzati da ciarlatani (da lì la denominazione 'snake-oil'). Molte di quelle compagnie non gradirono una tale definizione, e iniziarono a inviarmi minacciose missive legali.

La difesa migliore fu pubblicare quelle minacce come lettere a Crypto-Gram, anche se i miei legali me lo hanno sempre sconsigliato. Nessuno di questi incidenti si spinse mai oltre lo stadio della minaccia, anche se di tanto in tanto apparve qualche ingiunzione.

Negli anni, gli interessi principali di Crypto-Gram sono cambiati. Inizialmente non si parlava d'altro che di crittografia. Poi, sempre più sicurezza informatica e di rete. Poi (specialmente dopo l'11 settembre), la sicurezza più in generale: terrorismo, aerei, documenti d'identità, macchine per il voto, ecc. E adesso si parla più dell'economia e della psicologia della sicurezza. La mia carriera è stata una progressione dallo specifico al generale, e Crypto-Gram si è generalizzata per riflettere tale progressione.

L'altro cambiamento macroscopico riguardante Crypto-Gram avvenne nell'ottobre 2004. Mi ero documentato sui blog e sul blogging, e mi sono chiesto per diversi mesi se passare Crypto-Gram al formato blog fosse una buona idea oppure no. Ancora una volta si trattava di velocità e frequenza. Notai che altri commentavano le varie vicende di sicurezza con più rapidità, e che quando Crypto-Gram veniva pubblicato a metà del mese, molti avevano già linkato ad altre storie. Un blog mi avrebbe permesso una maggiore velocità nel pubblicare i miei commenti e di far parte dei dibattiti 'a caldo'.

Non riuscivo a decidermi. Molte persone mi consigliarono di cambiare, perché il blog era il formato del futuro. Ero scettico, e preferivo inviare la mia newsletter nelle caselle di posta dei miei lettori ogni mese. Mandai un sondaggio a 400 iscritti (200 scelti a caso e 200 persone che si erano iscritte il mese precedente). La soluzione finale fu la seconda cosa più intelligente da me pensata per questa newsletter: fare entrambe le cose, blog e newsletter.

Il blog "Schneier on Security" iniziò nella forma di articoli in stile Crypto-Gram, aggiornati quotidianamente. Così come i primi post avevano la stessa struttura degli articoli di Crypto-Gram, con i link in fondo. Nei mesi seguenti ho imparato qualcosa in più sullo stile di un blog, e i post hanno iniziato a essere presentati più propriamente come post di un blog. Ora il blog è il prodotto primario, e il 15 di ogni mese prendo i post del blog del mese precedente e li riconfiguro in formato Crypto-Gram. Anche oggi, la maggior parte dei lettori preferisce ricevere Crypto-Gram via email ogni mese, anche se leggono il blog online.

Attualmente a me piacciono entrambi. Mi piace l'immediatezza del blog, e mi piace il formato email di Crypto-Gram. E anche dopo dieci anni, continua a piacermi lo scrivere.

Spesso le persone mi chiedono dove trovo il tempo di scrivere così tanto. Per me è una domanda curiosa, perché scrivere è quel che adoro fare. Trovo il tempo a casa, mentre viaggio in aereo, nelle stanze d'albergo, dovunque. Lo scrivere per me non è un lavoro noioso o un onere (okay, forse a volte lo è), è qualcosa che mi rilassa. Mi piace buttar giù le mie idee in un flusso narrativo coerente. E non vi è nulla che mi dia più soddisfazione del fatto che poi la gente le legga.

Il feedback migliore che ricevo dai lettori è quando qualcuno mi scrive cose come "Hai cambiato il mio modo di pensare". È questo ciò che voglio fare. Voglio cambiare il modo in cui si pensa alla sicurezza. Voglio cambiare il modo di pensare sulle minacce, sui rischi e i compromessi, sui prodotti e i servizi di sicurezza, e sulla retorica che viene utilizzata per parlare di sicurezza in politica. Il fatto che siate d'accordo con me oppure no è di minore importanza. Quel che conta è che stiate pensando in modo diverso.

Grazie. In questo decimo anniversario voglio ringraziare tutti. Grazie a voi, lettori di lunga data, e a voi, nuovi iscritti e nuovi lettori. Grazie di continuare a leggere quel che ho da comunicare. Tutto questo per me è ancora divertente, interessante e stimolante. Spero che continui a esserlo anche per voi.

La pagina su Crypto-Gram, che comprende informazioni sulle traduzioni:
<<http://www.schneier.com/crypto-gram.html>>

I numeri arretrati di Crypto-Gram:
<<http://www.schneier.com/crypto-gram-back.html>>

Il primo post:
<http://www.schneier.com/blog/archives/2004/10/new_blog_and_ch.html>

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

Tecnologie a duplice uso e la questione di equità

Il 27 aprile 2007, l'Estonia è stata attaccata nel cyberspazio. A seguito di un incidente diplomatico con la Russia sul trasferimento di un monumento sovietico della Seconda Guerra Mondiale, le reti di molte organizzazioni estoni, fra cui il parlamento estone, banche, ministeri, giornali ed enti televisivi sono state attaccate e in molti casi messe fuori uso. L'Estonia ha immediatamente accusato la Russia, e la Russia ha immediatamente negato qualsiasi coinvolgimento.

Di questo caso si è parlato in termini sensazionalistici come della prima guerra cibernetica: la Russia che attacca l'Estonia nel cyberspazio. Ma a distanza di più di un anno non sono ancora emerse prove che il governo russo sia responsabile di tali attacchi denial-of-service. Malgrado gli hacker russi siano stati innegabilmente fra i maggiori istigatori dell'attacco, gli unici individui che sono stati identificati con certezza sono dei giovani di origine russa residenti in Estonia, irritati per l'incidente del monumento storico.

Quando non si è capaci di distinguere un attacco ostile da parte di un altro paese dall'opera di ragazzini annoiati spinti da motivazioni personali, allora è un bel problema.

Separare concetti quali guerra cibernetica, terrorismo cibernetico e crimine cibernetico non è facile, e di questi tempi occorre un segnapunti per differenziarli. Non è solo il fatto che è difficile rintracciare le persone nel cyberspazio, è che gli attacchi militari e civili (nonché le difese) si assomigliano.

Il termine tradizionale per la tecnologia che l'esercito condivide con i civili è "a duplice uso". A differenza di bombe a mano, carri armati e sistemi per il tracciamento di missili, le tecnologie a duplice uso hanno applicazioni sia militari che civili. Queste tecnologie a duplice uso erano solite essere delle eccezioni; persino cose che ci si aspetterebbe essere a duplice uso, come i sistemi radar e le toilette, venivano progettate in maniera diversa per i militari. Oggi però quasi tutta la information technology è a duplice uso. Entrambe le sfere, militare e civile, utilizzano gli stessi sistemi operativi, gli stessi protocolli di rete, le stesse applicazioni, persino il medesimo software di sicurezza.

E le tecnologie di attacco sono le stesse. La recente e improvvisa serie di hack mirati alle reti militari statunitensi, comunemente attribuiti alla Cina, sfruttano le stesse vulnerabilità e utilizzano le stesse tecniche degli attacchi criminali ai danni di reti aziendali. I worm che girano su Internet saltano nelle reti militari segrete in meno di 24 ore, anche se quelle reti sono fisicamente separate da Internet. Il Navy Cyber Defense Operations Command utilizza gli stessi strumenti contro le stesse minacce di una qualsiasi grossa compagnia.

Dato che aggressori e difensori ricorrono alla medesima tecnologia IT, esiste una tensione fondamentale fra attacco e difesa cibernetici. La National Security Agency si è riferita a questo fenomeno con il termine "equities issue", "questione di equità" e possiamo riassumerlo così: quando una entità militare scopre una vulnerabilità in una tecnologia a duplice uso, può agire in due modi. Può notificare il produttore e sistemare la vulnerabilità, proteggendo di conseguenza sia i buoni che i cattivi. Oppure può non rivelare la vulnerabilità, lasciando così a rischio sia i buoni che i cattivi.

La questione di equità è sempre stata dibattuta animosamente all'interno della NSA. In sostanza, la NSA ha due ruoli: intercettare dati e strumenti del nemico, e proteggere i nostri. Quando entrambe le parti si servono delle medesime cose, l'agenzia deve decidere se sfruttare le vulnerabilità per intercettare le cose altrui o chiudere quelle stesse vulnerabilità per proteggere le nostre cose.

Negli anni Ottanta e anche prima, la tendenza della NSA era quella di non divulgare le vulnerabilità. Negli anni Novanta la musica è cambiata, e la NSA ha iniziato ad aprirsi e ad aiutare tutti noi a migliorare le nostre difese di sicurezza. Ma dopo gli attacchi dell'11 settembre, la NSA è tornata sulle sue posizioni iniziali: le vulnerabilità dovevano essere raccolte in segreto. Lentamente, la corrente negli Stati Uniti sta di nuovo cambiando.

Adesso vediamo la NSA contribuire a rendere più sicuro Windows Vista e rilasciare una propria versione di Linux. Intanto, il Dipartimento per la Sicurezza Nazionale sta finanziando un progetto per proteggere i pacchetti software open source più diffusi, e nel Regno Unito il GCHQ sta scoprendo bug in PGPDisk e li sta notificando all'azienda produttrice. (Si dice che la NSA stia facendo lo stesso con BitLocker).

Sono assolutamente a favore di questa tendenza, perché la mia sicurezza aumenta gratuitamente. Ogni volta che la NSA trova un problema di sicurezza e fa in modo che il produttore lo sistemi, la sicurezza di tutti noi migliora. È un beneficio collaterale delle tecnologie a duplice uso.

Ma voglio che i governi facciano di più. Voglio che sfruttino il loro potere di acquisto per migliorare la mia sicurezza. Voglio che offrano in tutto il paese contratti per il software (di sicurezza e non) che abbiano specifici requisiti di sicurezza. Se questi contratti sono sufficientemente grossi, le aziende si impegneranno a modificare il loro prodotti perché soddisfino quei requisiti. E ancora una volta tutti noi trarremo vantaggio dalle migliori di sicurezza.

L'unico esempio che conosco di un tale modello è un concorso per l'ottenimento della crittografia per dischi rigidi full-disk encryption, ma è certamente possibile farlo con firewall, sistemi antintrusione, database, hardware di rete, persino con sistemi operativi.

Quando si tratta di tecnologie IT, la questione di equità dovrebbe essere una cosa semplicissima. Gli usi positivi del nostro hardware, del software, dei sistemi operativi, dei protocolli di rete e di tutto il resto superano di gran lunga gli usi negativi. È ora che il governo impieghi la propria immensa conoscenza ed esperienza, per non parlare del potere d'acquisto, per migliorare la sicurezza cibernetica per tutti noi.

La guerra cibernetica dell'Estonia:

<http://www.wired.com/politics/security/magazine/15-09/ff_estonia>
<<http://blog.wired.com/27bstroke6/2008/01/we-traced-the-c.html>>

Guerra cibernetica, terrorismo cibernetico, ecc.

<<http://www.schneier.com/blog/archives/2007/06/cyberwar.html>>

Le iniziative di sicurezza cibernetica della NSA e del Dipartimento per la Sicurezza Nazionale:

<http://www.schneier.com/blog/archives/2007/01/nsa_helps_micro_1.html>
<<http://www.nsa.gov/selinux/>>
<<http://www.eweek.com/c/a/Security/DHS-Funds-OpenSource-Security-Project/>>
oppure <<http://tinyurl.com/3ggg5g>>
<http://www.schneier.com/blog/archives/2007/01/us_government_t.html>

Questo articolo è originariamente apparso su Wired.com.

<http://www.wired.com/politics/security/commentary/securitymatters/2008/05/blog_securitymatters_0501>
oppure <<http://tinyurl.com/68zj7m>>

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

Attraversare le frontiere con computer portatili e PDA

Il mese scorso una corte statunitense ha stabilito che gli agenti di frontiera possono effettuare ricerche nel vostro portatile (o in qualsiasi altro dispositivo elettronico) quando entrate negli Stati Uniti. Possono requisirvi il computer e scaricarne l'intero contenuto, o trattenerlo per diversi giorni. Customs and Border Patrol non ha pubblicato alcuna regolamentazione riguardante questa pratica, e io ed altri abbiamo scritto una lettera al Congresso sollecitando un'investigazione e una regolamentazione di tale pratica.

Ma in questo gli Stati Uniti non sono soli. Gli agenti di frontiera britannici requisiscono i portatili per cercare contenuti pornografici. E su Internet si riferisce che questo genere di cose accade anche in altri paesi. Non vi piacerà, ma è un fatto. Come proteggersi, dunque?

Criptare l'intero disco rigido, una misura di sicurezza che dovrete sicuramente adottare in caso il vostro computer vada perso o venga rubato, non servirà in questa circostanza. L'agente di frontiera probabilmente inizierà tutta la procedura con un "Per favore, inserisca la password". Ovviamente potete rifiutarvi, ma questo porterà a ulteriori perquisizioni, potrebbero trattenervi ancor di più, rifiutare il vostro ingresso nel paese... Insomma, troveranno un modo per rovinarvi la giornata.

Dovrete nascondere i vostri dati. Fate in modo che una parte del disco rigido sia criptata con una chiave diversa (anche se avete già criptato l'intero disco rigido) e mantenete le informazioni sensibili in quella porzione di disco. Molti programmi vi permettono di farlo. Io utilizzo PGP Disk (www.pgp.com). Anche TrueCrypt (www.truecrypt.org) va bene, ed è gratis.

Gli agenti di frontiera potrebbero mettersi a cercare nel vostro portatile, ma sarà difficile che incontreranno la partizione criptata (come ulteriore misura cautelativa potreste renderne l'icona invisibile). E se scaricano i contenuti del disco rigido per esaminarli in un secondo momento, non avrete di che preoccuparvi.

Assicuratevi di scegliere una password crittografica forte. I dettagli sono troppo complicati per fornirvi un suggerimento veloce, ma sostanzialmente qualunque cosa facile da ricordare sarà anche facile da indovinare. Purtroppo questa non è la soluzione perfetta. Il vostro computer potrebbe aver lasciato una copia della password da qualche parte sul disco, e un software di analisi forense intelligente la troverà di certo.

La miglior difesa, pertanto, è di ripulire il portatile. Un agente di frontiera non può leggere quel che non avete. E non avete bisogno dell'archivio di email e di informazioni sui clienti degli ultimi cinque anni. Non vi servono vecchie lettere d'amore o certe foto (sapete di quali foto sto parlando). Cancellate qualunque cosa non vi serva assolutamente, e utilizzate un programma per la cancellazione sicura dei file. Già che ci siete, eliminate i cookie del browser, la cache e la cronologia. I siti Web che avete visitato non sono affari altrui. E spegnete il computer, non mettetelo in stop soltanto, prima di passare la frontiera; così facendo vengono cancellate altre cose. Pensate a tutto questo come ultima cosa da fare prima di metter via i vostri dispositivi elettronici quando vi preparate all'atterraggio. Alcune aziende ora forniscono ai propri dipendenti dei portatili forensicamente puliti per viaggiare, e permettono di scaricare le informazioni sensibili attraverso un Virtual Private Network una volta che i dipendenti sono entrati nel paese. Il lavoro svolto viene inviato con lo stesso sistema, e tutto viene cancellato prima di passare la frontiera per tornare a casa. È un'ottima idea se potete metterla in atto.

Se non vi è possibile, considerate il trasferimento dei vostri dati sensibili su una chiavetta USB o anche una scheda di memoria per fotocamera: anche le schede da 16 GB ormai hanno prezzi abbordabili. Criptate il tutto, naturalmente, perché è facile perdere un oggetto tanto piccolo. Mettetela in tasca, e con ogni probabilità non verrà nemmeno notata anche se l'agente di frontiera si mette a perquisirvi il portatile. Se viene scoperta, potete provare a dire: "Non so che cosa contiene. Il mio capo mi ha detto di consegnarla al direttore della sede di New York". Se avete scelto una password crittografica forte, non vi importerà se la confiscano.

Infine, non dimenticate il cellulare e il PDA. Gli agenti di frontiera possono esaminare anche quelli: le email, la rubrica contatti, l'agenda. Purtroppo l'unica cosa da fare in questo caso è cancellare quei dati.

Mi rendo conto che tutto questo suoni un po' laborioso, e che è più facile ignorare queste misure e sperare di non essere perquisiti. Oggi le probabilità giocano a vostro favore, ma grazie a nuovi strumenti d'analisi forense, le ricerche automatiche stanno diventando sempre più semplici, e il recente provvedimento stabilito da quella corte statunitense potrebbe incentivare altri paesi a fare altrettanto. Meglio stare sul sicuro.

I miei consigli sulla scelta di password sicure:

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

Questo articolo è originariamente apparso sul Guardian:

<<http://www.guardian.co.uk/technology/2008/may/15/computing.security>>

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

News

Ho già scritto in merito al RIPA (Regulation of Investigatory Powers Act) del Regno Unito, che è stato pubblicizzato come un mezzo per combattere il terrorismo e altri gravi crimini, quando poi è stato usato contro i sostenitori dei diritti degli animali. Le ultime notizie dal Regno Unito: un consiglio locale si è servito di alcuni provvedimenti di tale legge per mettere sotto sorveglianza una coppia di persone e i loro figli, per "sospette attività fraudolente in luoghi scolastici".

<<http://news.bbc.co.uk/1/hi/england/dorset/7341179.stm>>

<http://www.theregister.co.uk/2008/04/11/poole_council_ripa/>

<<http://news.bbc.co.uk/1/hi/england/dorset/7343445.stm>>

<http://www.schneier.com/blog/archives/2007/11/animal_rights_a.html>

Un ricercatore parla dell'intrinseca capacità degli esseri umani di fare del male:

<<http://www.independent.co.uk/news/people/maverick-academic-philip-zimbardo-says-we-are-all-capable-of-evil-is-he-right-789161.html>>

oppure <<http://tinyurl.com/36jqwh>>

Un confronto fra la sicurezza cibernetica e la sicurezza in mare aperto ai primi dell'Ottocento:

<<http://www.csoonline.com/article/print/329164>>

Di solito non perdo tempo a segnalare cose del genere, ma questa fuga di dati in Oklahoma è particolarmente grave. Chiunque con un minimo di conoscenze di SQL avrebbe potuto registrare qualsiasi persona avesse voluto come aggressore sessuale.

<<http://thedailywtf.com/Articles/Oklahoma-Leaks-Tens-of-Thousands-of-Social-Security-Numbers,-Other-Sensitive-Data.aspx>>

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

Foto divertenti di telecamere di sorveglianza:

<<http://www.flickr.com/photos/spiggycat/2393460671/in/pool-dcist/>>

<http://www.dailymail.co.uk/pages/live/articles/news/news.html?in_article_id=559547&in_page_id=1770>

oppure <<http://tinyurl.com/4rs34u>>

<<http://www.banksy.co.uk/outdoors/images/landscapes/camera-girl-4.jpg>>

<http://www.artofthestate.co.uk/photos/banksy_one_nation_under_CCTV_day.jpg>

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

Michael Chertoff, segretario della Sicurezza Nazionale, sostiene che le impronte digitali non sono dati personali.

<<http://thinkprogress.org/2008/04/16/chertoff-fingerprints/>>

Pare che stia confondendo dati segreti e dati personali. Molte informazioni personali non sono particolarmente segrete.

Sono stufo di sentire quella storia secondo cui la gente sarebbe disposta a rivelare le proprie password in cambio di una tavoletta di cioccolato. Non ho visto alcuna verifica che le password fornite siano vere. Io darei sicuramente una password fasulla in cambio di una tavoletta di cioccolato.

<<http://blogs.wsj.com/biztech/2008/04/16/security-is-no-match-for-chocolate-and-good-looking-women/?mod=WSJBlog>>

oppure <<http://tinyurl.com/6baob2>>

Un gioco sulla sicurezza aeroportuale:

<<http://www.shockwave.com/gamelanding/airportsecurity.jsp>>

La TSA vuole uno strumento per stimare i rischi delle reti di trasporto.

<<http://www.gsnmagazine.com/cms/resources/business-opportunities/701.html>>

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

Non credo sia necessario essere fra i migliori per qualificarsi. Un altro sistema automatizzato ha classificato Boise (Indiana) fra le città più vulnerabili. Dico semplicemente che la soglia da superare non è molto alta.

<<http://www.washingtonpost.com/wp-dyn/content/article/2008/04/04/AR2008040403022.html>>

oppure <<http://tinyurl.com/3nrudx>>

Questo genere di ricerca è interessante: data una patch di sicurezza, è possibile scoprire automaticamente mediante reverse-engineering la vulnerabilità di sicurezza che viene sistemata e creare codice di exploit per sfruttarla? Pare proprio di sì.

<<http://www.cs.cmu.edu/~dbrumley/pubs/apeg.html>>

Hackerare le pagine di errore dei provider Internet. Questo è grave.

<<http://blog.wired.com/27bstroke6/2008/04/isps-error-page.html>>

<http://www.theregister.co.uk/2008/04/20/kaminsky_demo_at_toorcon/>

Questo scritto ha vinto il titolo di miglior studio al primo Workshop USENIX sugli exploit su vasta scala e sulle minacce emergenti (Large-Scale Exploits and Emergent Threat); parla della progettazione malevola di processori in modo che supportino l'hacking:

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

Teoria? Certo. Ma combiniamola con storie di hardware contraffatto proveniente dalla Cina, ed ecco all'orizzonte un problema potenzialmente molto grave.

<<http://www.hardwareanalysis.com/content/article/1874/made-in-china-security-risk/>>

oppure <<http://tinyurl.com/3ukoap>>

Un elenco di persone decedute, stilato per evitare furti di identità, viene utilizzato per commettere un furto d'identità.

<<http://blog.wired.com/27bstroke6/2008/04/feds-charge-cal.html>>

Proteggere lo schermo del proprio portatile da occhi indiscreti: una soluzione low-tech:

<<http://www.engadget.com/2008/04/16/the-body-laptop-interface-is-knitted-from-thneed-which-nobody-n/>>

oppure <<http://tinyurl.com/3s525l>>

Una professione noiosa intorpidisce la mente. Lo si sapeva, ma è meglio insistere.
<<http://news.bbc.co.uk/2/hi/science/nature/7358863.stm>>

Questo video dimostra il nocciolo della questione ottimamente.
<<http://www.youtube.com/watch?v=Ahg6qcgoy4>>

Interessante articolo d'investigazione di Business Week sullo spionaggio cibernetico cinese contro il governo USA e la reazione del governo.

<http://www.businessweek.com/magazine/content/08_16/b4080032218430.htm>

Sarà mai vinta la guerra ai fotografi?

<<http://www.memphisflyer.com/memphis/Content?oid=oid%3A41348>>

Il sequestro virtuale è un reato riconosciuto in Messico:

<<http://www.nytimes.com/2008/04/29/world/americas/29mexico.html>>

Questa immagine, che dimostra un attacco di iniezione di codice SQL contro gli scanner automatici di targhe automobilistiche, è quasi certamente ritoccata con Photoshop, ed è uno scherzo, ma è senza dubbio un'idea brillante. Con il continuo aumento di questo tipo di scanner, perché no?

<<http://www.areino.com/hackeando/>>

<<http://www.schneier.com/essay-057.html>>

Mi ricorda questa vignetta di xkcd:

<<http://xkcd.com/327/>>

"Neighborhood Watch": divertente presa in giro del Dipartimento per la Sicurezza Nazionale:

<<http://dhsnnw.org/index.html>>

<http://itp.nyu.edu/blogs/ecm292_thesis/>

Microsoft sta distribuendo una chiavetta USB piena di strumenti Windows di analisi forense per la polizia:

<http://www.schneier.com/blog/archives/2008/04/microsoft_has_d.html>

Eroina contro terrorismo: un articolo interessante sui compromessi di sicurezza.

<http://www.timesonline.co.uk/tol/comment/columnists/guest_contributors/article3835351.ece>

oppure <<http://tinyurl.com/59j2qj>>

Un articolo mordace su ciò di cui bisogna preoccuparsi:

<<http://tencartrain.com/?p=627>>

Nomi di sky marshal sulla no-fly list. Se non fosse così triste, sarebbe divertente.

<http://www.washingtontimes.com/apps/pbcs.dll/article?AID=/20080429/NATION/782525487/-1/RSS_NATION_POLITICS>

oppure <<http://tinyurl.com/4fbzu2>>

<http://www.economist.com/blogs/gulliver/2008/05/that_pesky_nofly_list.cfm>

oppure <<http://tinyurl.com/3uw9ak>>

Ho appena ricevuto per posta la seconda edizione di "Security Engineering" di Ross Anderson. È fantastico. Si tratta del libro migliore in circolazione sull'argomento, e lo consiglio a chiunque lavori in questo campo. E non solo perché ne ho scritto la

prefazione. Potete scaricare l'introduzione e sei capitoli (o anche l'intera prima edizione).

<http://www.amazon.com/Security-Engineering-Building-Dependable-Distributed/dp/0470068523/ref=pd_bbs_sr_2?ie=UTF8&s=books&qid=1209409426&sr=8-2>

oppure <<http://tinyurl.com/4prdy2>>

<<http://www.cl.cam.ac.uk/~rja14/bruce.html>>

<<http://www.cl.cam.ac.uk/~rja14/book.html>>

Il Dipartimento di Stato USA smarrisce centinaia di portatili. Scommetto qualsiasi cosa che non erano criptati.

<<http://www.cqpolitics.com/wmspage.cfm?parm1=5&docID=hsnews-000002716318>>

oppure <<http://tinyurl.com/66ovev>>

Le telecamere di sicurezza a Londra non riducono il tasso di criminalità. La cosa, ovviamente, non sorprende.

<<http://news.bbc.co.uk/1/hi/uk/7384843.stm>>

<<http://www.guardian.co.uk/uk/2008/may/06/ukcrime1>>

<http://www.schneier.com/blog/archives/2008/05/londons_cameras_1.html>

La minaccia di Al Qaeda è sopravvalutata:

<<http://www.newsweek.com/id/135654/>>

Ricordate i due uomini che stavano esibendo un "comportamento anomalo" su un traghetto dello stato di Washington la scorsa estate? Beh, si trattava di turisti, non di terroristi.

<http://www.schneier.com/blog/archives/2008/05/tourists_not_te_1.html>

Eccellente articolo che delinea la cronaca del dibattito USA sulla sorveglianza, dalla metà degli anni Ottanta ai giorni nostri. Non aspettatevi una buona copertura del dibattito attuale, però: la legalità del recente programma di intercettazione nazionale della NSA, e la legalità dell'assistenza fornita dalle grandi aziende di telecomunicazioni.

<<http://www.govexec.com/dailyfed/0408/042208nj1.htm>>

Comoda guida sull'utilizzo del cellulare come strumento per spiare:

<<http://www.geeksaresexy.net/2008/05/05/cell-phone-spying-is-your-life-being-monitored/>>

oppure <<http://tinyurl.com/5adjr6>>

Non so che pensare di Sweet Dreams Security e dei suoi sforzi per rendere la sicurezza 'affettuosa'.

<<http://www.deardad.net/sds-html/>>

<http://www.schneier.com/blog/archives/2008/05/making_security.html>

Il terrorismo come tassa: di sicuro un buon modo di considerarlo.

<http://www.schneier.com/blog/archives/2008/05/terrorism_as_a.html>

Una richiesta di brevetto interessante da parte di Microsoft: Guardian Angel.

<[http://appft1.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PG01&p=1&u=%2Fnethtml%2FPTO%2Fsrchnum.html&r=1&f=G&l=50&s1=%2220080082465%22.PG.NR.&OS=DN/20080082465&RS=DN/20080082465"](http://appft1.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PG01&p=1&u=%2Fnethtml%2FPTO%2Fsrchnum.html&r=1&f=G&l=50&s1=%2220080082465%22.PG.NR.&OS=DN/20080082465&RS=DN/20080082465)>

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

Notare che Bill Gates e Ray Ozzie sono co-inventori.

Il Dipartimento per la Sicurezza Nazionale ha varato una nuova iniziativa da 200 milioni di dollari: CNCI (Comprehensive National Cybersecurity Initiative). Il Congresso è lieto di finanziarla, ma vorrebbe sapere a che cosa serve. Devo ammettere di essere curioso anch'io.

<<http://blog.wired.com/27bstroke6/2008/05/senate-panel-qu.html>>

<<http://arstechnica.com/news.ars/post/20080506-senators-press-dhs-head-for-details-on-cybersecurity-plans.html>>

La U.S. Air Force sta considerando la creazione di un proprio botnet. In realtà credo sia una buona idea, almeno finché si servono di computer che possiedono legalmente.

<<http://www.armedforcesjournal.com/2008/05/3375884>>

<<http://arstechnica.com/news.ars/post/20080512-preparing-for-cyber-warfare-us-air-force-floats-botnet-plan.html>>

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

Il vincitore del Terzo Concorso "Minaccia da Trama Cinematografica"

Il 7 aprile (con sette giorni di ritardo) ho annunciato sul mio blog la terza edizione del concorso "Minaccia da Trama Cinematografica":

"L'obiettivo di questa terza edizione del concorso è creare paura. Non un terrore generico, ma una paura che si può attenuare grazie alla vendita del vostro nuovo prodotto. Esistono parecchi rischi là fuori, alcuni molto seri, altri talmente improbabili che non dovremmo neanche preoccuparci, altri ancora completamente inventati. Ed esistono svariati prodotti che forniscono sicurezza contro tali rischi.

"Il vostro compito è inventarne uno. Prima di tutto, trovate un rischio o createne uno. Può essere una minaccia terroristica o criminale, il pericolo di una calamità naturale, o un semplice rischio domestico, qualunque cosa. Più è bizzarro, meglio è. Poi create un prodotto che tutti DEVONO comprare per forza se vogliono proteggersi da tale minaccia. E infine scrivete un annuncio pubblicitario per quel prodotto.

"Ogni proposta ha un limite di 150 parole (l'esempio citato era di 97 parole), perché la paura non richiede molte parole di spiegazione. Diteci perché dovremmo avere paura e perché dovremmo acquistare il vostro prodotto."

Il 7 maggio ho pubblicato i cinque finalisti scelti fra 327 commenti sul blog:

- * Adulterometro di DNA per rilevare se un cameriere sputa nella vostra zuppa.
- * Strisce di test per dentifricio.
- * Dispositivo SOS per persone chiuse nei bagagliai delle auto.
- * Occhiali anti puntatore laser.

* Monitor di pulsazioni cardiache per misurare il livello di prontezza e vigilanza di un individuo.

Purtroppo, due di questi cinque contributi superavano il limite di 150 parole. Dei tre rimanenti, con l'aiuto dei miei lettori, ho scelto il vincitore.

Vi presento il vincitore della Terza Edizione del Concorso "Minaccia da Trama Cinematografica", Aaron Massey:

"Tommy Tester Toothpaste Strips:
[Strisce di test per dentifricio]

"Molti americani furono scandalizzati nel conoscere i risultati delle prove di ricerca sui metalli pesanti e la pasta dentifricia condotte dal New England Journal of Medicine, che la FDA sta cercando di confermare soltanto ora. Quest'ultimo spauracchio segue le centinaia di decessi collegati alla contaminazione della pasta dentifricia con glicoeetilene, una sostanza chimica utilizzata negli antigelo potenzialmente pericolosa.

"Alla luce di questo rischio continuato per la salute, gli Hamilton Health Labs sono orgogliosi di annunciare Tommy Tester Toothpaste Strips! Basta applicare un po' di dentifricio di un tubetto appena aperto sulla striscia e lasciarlo riposare tre minuti. È così semplice! Se la striscia diventa di colore blu, il tubetto di dentifricio è innocuo e potrete usarlo tranquillamente. Se invece la striscia diventa rosa, gettate immediatamente il dentifricio e chiamate il numero di emergenza della FDA: 301-443-1240.

"Non lasciate che la vostra famiglia diventi un altro caso statistico quando la soluzione costa soltanto 2,95 dollari!"

Aaron vince... beh, non vince nulla a parte la fama e la gloria che gli possono offrire Crypto-Gram e il mio blog. Diamogli allora la fama e la gloria che si merita. Congratulazioni.

L'annuncio:

<http://www.schneier.com/blog/archives/2008/04/third_annual_mo.html>

I semifinalisti:

<http://www.schneier.com/blog/archives/2008/05/third_annual_mo_2.html>

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

La RSA Conference

La scorsa settimana si è tenuta la RSA Conference, senza dubbio la più grande conferenza di information security del mondo. Più di 17.000 persone sono affluite al Moscone Center di San Francisco per assistere ad alcuni dei 250 incontri, per partecipare a innumerevoli party, e cercando di evitare più di 350 espositori che facevano a gara per vendere loro qualche prodotto.

Se interpellate gli espositori, tuttavia, la lamentela più comune è che i visitatori non acquistano.

Non è la qualità di ciò che viene venduto. Il padiglione delle esposizioni è pieno di nuovi prodotti di sicurezza, nuove tecnologie e nuove idee. Molte di queste sono soluzioni che renderanno le aziende dei visitatori molto più sicure sotto vari punti di vista. Il problema è che la maggior parte delle persone che partecipano alla RSA Conference non riescono a capire che cosa fanno tali prodotti e perché dovrebbero comprarli. E quindi non comprano.

Ho parlato con una persona il cui viaggio veniva pagato da una impresa di sicurezza piuttosto piccola. Era uno dei primi clienti di quella compagnia, e la compagnia era orgogliosa di farlo apparire davanti alla stampa. Gli ho chiesto se aveva fatto un giro nel padiglione delle esposizioni, cercando le aziende concorrenti per vedere se vi fosse qualche vantaggio nel cambiare prodotto.

“Non riesco a capire di che si occupano tutte quelle aziende”, mi ha risposto.

Gli credo. Gli stand sono zeppi di dichiarazioni generali sul prodotto, banalità senza senso sulla sicurezza, e incomprensibile letteratura di marketing. Potreste entrare in uno stand, ascoltare uno sproloquio di cinque minuti di un venditore, e continuare a non avere idea del prodotto che quella azienda vuole vendere. Persino i professionisti di sicurezza più esperti sono confusi.

Il commercio richiede un allineamento mentale fra compratore e venditore, e qui semplicemente non accade. I venditori non riescono a spiegare ai compratori che cosa stanno vendendo, e i compratori non comprano perché non capiscono ciò che i venditori stanno vendendo. Non vi è corrispondenza fra le due parti, che sono così lontane da parlare appena la stessa lingua.

Ciò è negativo nel breve termine (alcune ottime compagnie finiranno in bancarotta e alcune tecnologie di sicurezza molto buone non verranno implementate), ma è un'ottima cosa a lungo termine. Dimostra che l'industria informatica sta maturando: l'IT sta diventando complicata e astrusa, e gli utenti stanno iniziando a trattarla come un'infrastruttura.

È già da qualche tempo che ho previsto la morte dell'industria della sicurezza. Non la fine dell'information security come requisito vitale, naturalmente, ma la fine dell'industria della sicurezza dell'utente finale, che si raduna alla RSA Conference. Quando qualcosa diventa infrastruttura (l'energia, l'acqua, il servizio di pulizia, la preparazione delle tasse, ecc.) ai clienti importano meno i dettagli e preferiscono i risultati. Le innovazioni tecnologiche diventano qualcosa a cui i fornitori di infrastruttura prestano attenzione, e la "impacchettano" per i propri clienti.

Nessuno vuole comprare la sicurezza. Si vuole acquistare qualcosa di veramente utile (sistemi di gestione dei database, strumenti di collaborazione per il Web 2.0, una rete aziendale) e lo si vuole sicuro. Nessuno vuole dover diventare un esperto di sicurezza IT. Nessuno vuole trovarsi obbligato a recarsi alla RSA Conference. Questo è il futuro della sicurezza IT.

Lo potete constatare nei grandi contratti di outsourcing IT che le aziende stanno firmando. Non contratti per l'outsourcing della sicurezza, ma contratti IT più generali

che comprendono anche la sicurezza. Lo potete constatare osservando l'attuale ondata di consolidamento industriale: non vi sono grandi compagnie di sicurezza che acquisiscono piccole imprese di sicurezza, ma compagnie che non si occupano di sicurezza che acquisiscono aziende di sicurezza. E lo potete vedere anche nella nuova popolarità del software come servizio: i clienti vogliono delle soluzioni, non vogliono preoccuparsi dei dettagli.

Vi immaginate se l'inventore del sistema frenante ABS (o di qualsiasi funzionalità di sicurezza di un'autovettura) dovesse venderlo direttamente al cliente? Sarebbe una difficile battaglia per convincere il guidatore medio che ha bisogno di un tale sistema; forse la tecnologia avrebbe avuto comunque successo, forse no. Ma non funziona così. Il sistema ABS, gli airbag, e quel sensore di prossimità tanto fastidioso che inizia a suonare quando in retromarcia vi avvicinate troppo a un ostacolo, vengono venduti alle case costruttrici di automobili, che li includono nelle auto poi vendute ai consumatori. Ciò non significa che la sicurezza di un'automobile non sia importante, anzi spesso queste nuove funzionalità vengono esaltate dalle stesse case costruttrici.

La RSA Conference non scomparirà, ovviamente. La sicurezza è troppo importante. Continueranno a esservi nuove tecnologie, nuovi prodotti e nuove imprese. Ma diventerà qualcosa che guarda verso l'interno, e si trasformerà lentamente in una conferenza industriale. Parteciperanno le aziende di sicurezza che vendono alle compagnie che a loro volta vendono agli utenti aziendali e domestici, e non sarà più una conferenza con 17.000 visitatori.

"Death of the Security Industry" [Fine dell'industria della sicurezza]:

<<http://www.schneier.com/essay-196.html>>

Consolidamento industriale:

<<http://www.schneier.com/essay-209.html>>

Commenti:

<http://www.computerweekly.com/blogs/david_lacey/2008/05/we_cant_have_enough_security_p_1.html>

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

Questo articolo è originariamente apparso su Wired.com.

<http://www.wired.com/politics/security/news/2008/04/securitymatters_0417>

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

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

Preferenze di rischio negli scimpanzé e nei bonobo

Ho già parlato della prospect theory, che spiega come le persone affrontano il rischio. Si tende a essere avversi al rischio quando si tratta di guadagni, e si ricerca il rischio quando si tratta di perdite:

"Da un punto di vista evolutivo, presumibilmente è una strategia di sopravvivenza migliore (a meno di imprevisti, naturalmente) accettare piccoli guadagni invece di rischiarli per ottenere guadagni maggiori, e rischiare grosse perdite invece di accettare

perdite di minor entità. I leoni inseguono gnu giovani o feriti perché l'investimento necessario per ucciderli è più basso. Prede più mature e in salute sarebbero forse più nutrienti, ma vi è il rischio di saltare completamente il pranzo se tali prede riuscissero a fuggire. E un pasto, anche piccolo, aiuterà il leone a tirare avanti un altro giorno. Arrivare in fondo alla giornata di oggi è più importante della possibilità di avere cibo domani.

"Analogamente, da un punto di vista evolutivo è meglio rischiare una perdita più grande che non accettarne una minore. Dato che gli animali tendono a vivere sul filo del rasoio tra fame e riproduzione, ogni perdita di cibo, grande o piccola, può essere qualcosa di grave. Ossia, in entrambi i casi il rischio è la morte. Se questo è vero, la scelta migliore è rischiare tutto senza aver nulla da perdere".

Questo comportamento è stato osservato anche negli animali: "varie specie di insetti, di uccelli e di mammiferi passano da una posizione neutrale nei confronti del rischio, a essere avversi al rischio quando compiono decisioni riguardanti le quantità di cibo, ma sono favorevoli al rischio in caso di ritardi nel ricevere cibo".

Uno studio recente analizza le preferenze relative di rischio in due specie molto simili: scimpanzé e bonobo. "Animali umani e non umani tendono a evitare situazioni rischiose. Se tali pattern di scelta economica sono adattabili, le preferenze di rischio dovrebbero riflettere gli ambienti tipici decisionali affrontati dagli organismi. Tuttavia, questo approccio non è stato largamente utilizzato per analizzare la sensibilità al rischio in specie strettamente imparentate con ecologie diverse. Qui abbiamo esaminato sperimentalmente il comportamento sensibile al rischio negli scimpanzé (*Pan troglodytes*) e nei bonobo (*Pan paniscus*), due specie strettamente legate le cui distinte ecologie si pensa siano la maggiore forza selettiva che dà forma ai loro peculiari repertori comportamentali. Dato che gli scimpanzé sfruttano risorse di cibo più rischiose in natura, la nostra previsione è stata che avrebbero esibito una tolleranza maggiore al rischio nelle scelte riguardanti il cibo. I risultati hanno confermato questa previsione: gli scimpanzé hanno preferito decisamente l'opzione rischiosa, mentre i bonobo hanno preferito l'opzione prestabilita. Tali risultati offrono un esempio relativamente raro di comportamento tendente al rischio nel contesto dei guadagni e mostrano come pressioni ecologiche possano influenzare il processo decisionale economico".

La tesi fondamentale è che nell'ambiente naturale dello scimpanzé, se non si corrono dei rischi, non si ottengono ricompense di alto valore (es. carne di scimmia). I bonobo "si affidano molto di più degli scimpanzé alla vegetazione erbacea terrestre, una risorsa di cibo più costante nello spazio e nel tempo". Pertanto è meno probabile che gli scimpanzé evitino di esporsi a rischi.

Tutto molto affascinante, ma vi sono almeno un paio di problemi con questo studio. Il primo lo spiegano i ricercatori nello studio stesso. Gli animali esaminati (cinque per ogni specie) provenivano dal Wolfgang Koehler Primate Research Center dello Zoo di Lipsia, e gli sperimentatori non sono stati in grado di stabilire differenze nelle "esperienze, culture e condizioni dei due gruppi specifici qui analizzati".

Il secondo problema è più generale: sappiamo molto poco della vita dei bonobo allo stato naturale. Esistono molti stereotipi popolari sui bonobo, ma sono piuttosto approssimativi.

In ogni caso, mi piace vedere questo tipo di ricerca: davvero affascinante.

Il post sul mio blog:

<http://www.schneier.com/blog/archives/2008/04/risk_preference.html>

<<http://journals.royalsociety.org/content/hj235725w4pp2872/?p=dca3144c481b44358c2fed990c973bc4&pi=5>>

oppure <<http://tinyurl.com/4w9p2w>>

La prospect theory:

<<http://www.schneier.com/essay-155.html>>

I bonobo allo stato naturale:

<http://www.newyorker.com/reporting/2007/07/30/070730fa_fact_parker>

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

Le news su Schneier/BT Counterpane

Audio e video dell'intervento di Schneier all'InfoSecurity Europe sulla riconcettualizzazione della sicurezza ("Reconceptualizing Security") o forse sul Teatro della Sicurezza ("The Theater of Security"):

<http://www.yada-yada.co.uk/podcasts/ReedExhibitions/InfosecurityEurope/audio/Hall_of_Fame_BruceSchneier.mp3>

oppure <<http://tinyurl.com/4x2j5a>>

<<http://www.yada-yada.co.uk/podcasts/ReedExhibitions/InfosecurityEurope/video/BruceSchneier.html>>

oppure <<http://tinyurl.com/44vyww>>

Schneier è stato intervistato alla radio olandese. L'introduzione e le domande sono in olandese, ma le risposte sono in inglese.

<http://www.xs4all.nl/~herbertb/2000+/Radio/BNR-eeuw/2008/eeuw_20080424_Veiligheid_bestaat_niet.mp3>

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

Schneier è stato intervistato dalla Anti War Radio. Si è trattato di una strana intervista, partita dall'articolo "Ritratto del Terrorista Moderno da Idiota" per poi muoversi verso il ruolo del governo di contro alle aziende in ambito di sicurezza.

<<http://antiwar.com/radio/2008/04/11/bruce-schneier/>>

Questa intervista a Schneier è stata condotta su video anche se viene presentata come testo, per cui non si legge bene come altre che ho svolto via email.

<http://computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security_hardware_and_software&articleId=9079720&taxonomyId=145&intsrc=kc_fe>

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

Un'altra intervista a Schneier, effettuata alla RSA Conference:

<http://techwebtv.feedroom.com/?fr_story=f0d0cf13252829540dc4e42104b05fe45d9043ca&rf>

oppure <<http://tinyurl.com/46st9s>>

Video-intervista a Schneier dal Regno Unito:

<<http://www.computerweekly.com/Articles/2008/04/30/230486/video-security-experts-bruce-schneier-and-ray-stanton-on-the-human-side-of.htm>>

oppure <<http://tinyurl.com/628amx>>

Due video-interviste a Schneier dall'Australia:

<<http://www.builderau.com.au/video/soa/Schneier-The-problem-of-evaluating-risk/0,2000064338,22441085p,00.htm>>

oppure <<http://tinyurl.com/4ua3k5>>

<<http://www.builderau.com.au/video/soa/Schneier-The-drama-of-security/0,2000064338,22441082p,00.htm>>

oppure <<http://tinyurl.com/4qz3c9>>

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

Il Canile: Passwordsafe.com

Non si tratta del mio Password Safe, ma di passwordsafe.com. Password Safe è un'applicazione open source che una volta caricata sul computer serve a criptare le password. Passwordsafe.com vi permette di conservare le vostre password sui suoi server. E promette di non guardarle.

"Posso fidarmi di PasswordSafe? Come abbiamo detto, ogni funzione è automatizzata, nessuno vede mai le vostre informazioni dato che vengono trattate dai programmi e poi criptate nel database. Vi ricordiamo ancora una volta che non consigliamo di conservare informazioni sensibili su PasswordSafe. Internamente, abbiamo utilizzato questo servizio per molti siti, programmi di creazione banner, programmi di affiliazione, servizi di email gratuita e molto altro".

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

Il mio Password Safe:

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

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

L'etica della ricerca delle vulnerabilità

Il metodo standard per ottenere il controllo del computer di qualcun altro è quello di sfruttare una vulnerabilità di un software presente su di esso. Ciò valeva negli anni Sessanta, quando i buffer overflow vennero utilizzati per la prima volta per attaccare i computer. Valeva nel 1988 quando il worm Morris fece leva su una vulnerabilità di Unix per attaccare i computer su Internet, ed è ancora alla base del funzionamento di molto malware moderno.

Le vulnerabilità sono errori software: errori nella specificazione e nel design, ma soprattutto errori di programmazione. Un qualsiasi pacchetto software corposo e sofisticato conterrà migliaia di questi errori. Tali vulnerabilità rimangono sopite nei nostri sistemi software, e aspettano di essere scoperte. Una volta scoperte, possono venire utilizzate per attaccare computer e sistemi. Questa è la base del patching di sicurezza: eliminare le vulnerabilità note. Ma molti sistemi non vengono riparati con patch di sicurezza, pertanto Internet è piena di vulnerabilità conosciute e sfruttabili.

Le nuove vulnerabilità sono beni molto ambiti. Un hacker che ne scopre una può venderla al mercato nero, ricattare il produttore minacciando la divulgazione, o semplicemente pubblicarla senza preoccuparsi delle conseguenze. E anche se non fa nessuna di queste cose, il semplice fatto che la vulnerabilità è nota a qualcuno fa aumentare il rischio per tutti gli utenti di quel software. Detto questo, è etico ricercare nuove vulnerabilità?

Sì, inequivocabilmente. Malgrado i rischi, la ricerca delle vulnerabilità è estremamente preziosa. La sicurezza è un abito mentale, e cercare vulnerabilità arricchisce tale abito mentale. Se neghiamo ai professionisti questo strumento di apprendimento essenziale, la sicurezza ne soffrirà di conseguenza.

Gli ingegneri di sicurezza vedono il mondo in maniera diversa dagli altri ingegneri. Invece di concentrarsi su come funzionano i sistemi, loro si concentrano su come i sistemi sbagliano, su come sia possibile indurli all'errore, e su come prevenire tali avarie e come proteggersi da esse. Moltissime vulnerabilità software non appaiono mai durante normali operazioni, solo quando un aggressore le sfrutta deliberatamente. Per cui gli ingegneri di sicurezza devono pensare come aggressori.

Le persone che non hanno questa mentalità a volte pensano di poter progettare prodotti di sicurezza, ma non ne sono capaci. E i risultati si possono vedere ovunque nella nostra società: nella crittografia da ciarlatani, nel software, nei protocolli Internet, nelle macchine per il voto, nelle macchine per il pagamento automatico e in altri sistemi di pagamento. Molti di tali sistemi avevano qualcuno incaricato di occuparsi della "sicurezza", ma non era qualcuno che avesse la mentalità dell'aggressore.

Questa mentalità è difficile da insegnare, e può essere innata o meno. Ma per allenare chi la possiede, è necessario che tali persone ricerchino e trovino le vulnerabilità di sicurezza, continuamente. E ciò è vero a prescindere dal settore di competenza. I crittografi in gamba scoprono le vulnerabilità negli algoritmi e nei protocolli altrui. Validi esperti di sicurezza del software scoprono vulnerabilità nel codice altrui. Validi progettisti di sicurezza aeroportuale scoprono nuovi metodi per aggirare la sicurezza in aeroporto. E così via.

Tutto ciò è talmente importante che quando qualcuno mi mostra un progetto di sicurezza realizzato da una persona che non conosco, la mia prima domanda è "Che cosa ha compromesso o violato il progettista?". Chiunque può ideare un sistema di sicurezza che non è in grado di superare e violare. Pertanto, quando qualcuno annuncia "Ecco il mio sistema di sicurezza, e non sono in grado di sconfiggerlo", la vostra prima reazione dovrebbe essere "Ma chi è lei?". Se è qualcuno che ha superato decine di sistemi simili, vale la pena dare un'occhiata al suo progetto. Se non è mai riuscito a violare alcunché, le possibilità che tale sistema sia valido sono nulle.

La ricerca delle vulnerabilità è essenziale perché rappresenta l'allenamento per la nostra prossima generazione di esperti di sicurezza informatica. Certo, nuove vulnerabilità scoperte nei software e negli aeroporti ci mettono a rischio, ma ci forniscono anche delle informazioni più realistiche sulla vera efficacia della sicurezza in atto. E certo, esistono metodi più o meno responsabili, e più o meno legali, di gestire una nuova vulnerabilità. Ma i "cattivi" sono sempre alla ricerca di nuove vulnerabilità, e se vogliamo avere qualche speranza di proteggere i nostri sistemi, dobbiamo fare in modo che i "buoni" siano almeno altrettanto competenti. Per me la questione non è se sia etico svolgere ricerche di vulnerabilità. Se qualcuno ha la capacità di analizzare e di fornire migliori intuizioni sul problema, la questione diventa, per lui, se sia etico o meno NON svolgere ricerche di vulnerabilità.

Questo articolo è originariamente apparso su InfoSecurity Magazine come parte di un 'botta e risposta' con Marcus Ranum. Potete leggere l'intervento di Marcus qui:

<http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1313268,00.html>

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

I nostri dati, noi stessi

Nell'era dell'informazione, tutti lasciamo un'ombra di dati.

Ovunque andiamo, lasciamo una traccia di informazioni. Non sono soltanto i nostri conti bancari e i portafogli azionari, o le bollette e gli estratti conto, che elencano ogni acquisto effettuato con carta di credito e ogni telefonata fatta. Ma anche il Telepass, le tessere-fedeltà dei supermercati, i bancomat, e così via.

Sono anche le nostre vite. Le nostre lettere d'amore e le chiacchierate fra amici. Le nostre email e i nostri messaggi SMS privati. I nostri business plan, le strategie e le conversazioni casuali. Le nostre simpatie e posizioni politiche. E queste sono soltanto le informazioni con cui interagiamo. Tutti noi abbiamo un'ombra che vive nelle banche dati di centinaia di aziende broker di informazioni; dati che ci riguardano, che sono sorprendentemente personali e paurosamente completi, a parte gli errori che non possiamo né vedere né correggere.

Quel che accade ai nostri dati, accade a noi stessi.

Questa nostra ombra non giace senza far nulla: viene continuamente toccata, esaminata, giudicata. Quando facciamo richiesta di un prestito bancario, sono i nostri dati che determineranno la risposta positiva o negativa della banca. Quando cerchiamo di imbarcarci su un aereo, sono i nostri dati che stabiliranno quanto approfonditamente verremo perquisiti, o se ci sarà data la possibilità di imbarcarci. Se il governo vuole indagare su di noi, è più probabile che passerà al setaccio i nostri dati che non le nostre dimore; e per molte di quelle informazioni non è nemmeno necessario un mandato.

Chi controlla i nostri dati, controlla le nostre vite.

È vero. Chiunque controlli i nostri dati può decidere se possiamo avere un prestito, se possiamo viaggiare in aereo, se possiamo recarci in un altro paese. O che tipo di sconto

possiamo ottenere da un commerciante, o persino come veniamo trattati dal servizio clienti. Un potenziale datore di lavoro può esaminare (illegalmente negli Stati Uniti) la nostra storia medica e decidere se offrirci o meno un posto. La polizia può raccogliere i nostri dati e decidere se rappresentiamo un rischio terroristico. Se un criminale riesce a procurarsi una sufficiente quantità di informazioni, può aprire carte di credito a nostro nome, prelevare denaro dai nostri investimenti, persino vendere la nostra proprietà. Il furto di identità è la prova estrema che il controllo dei nostri dati significa controllare la nostra vita.

Dobbiamo riprenderci i nostri dati.

I nostri dati sono una parte di noi, intima e personale, e su di essa abbiamo dei diritti fondamentali. Dovrebbero essere protetti da manipolazioni indesiderate.

Abbiamo bisogno di una legge esaustiva sulla privacy dei dati. Questa legge dovrebbe proteggere tutte le informazioni su di noi, senza limitarsi ai dati finanziari o medici. Dovrebbe limitare la capacità altrui di comprare o vendere le informazioni a nostra insaputa e senza il nostro consenso. Ci dovrebbe permettere di vedere quali informazioni su di noi sono in mano ad altri, e correggere eventuali errori e imprecisioni. Dovrebbe impedire al governo di andare a caccia dei nostri dati senza una supervisione giudiziaria. Dovrebbe far rispettare la cancellazione dei dati e limitare la raccolta di informazioni ove necessario. E abbiamo bisogno di qualcosa in più che semplici sanzioni simboliche per punire chi trasgredisce intenzionalmente.

È chiedere troppo, lo so, e ci vorranno anni prima di arrivare a quel punto. È facile non fare nulla e lasciare che il mercato abbia la meglio. Ma come si può vedere con cose quali le tessere-fedeltà delle drogherie e politiche di privacy che si accettano con un solo clic su molti siti Web, la maggior parte delle persone non ha idea di quanto la propria privacy venga violata, oppure non ha altra scelta. E le imprese, ovviamente, sono ben felici di raccogliere, comprare e vendere le nostre informazioni più sensibili. Ma gli effetti a lungo termine di tutto questo sulla società sono tossici: rinunciamo al controllo di noi stessi.

Questo articolo è originariamente apparso su Wired.com.

<http://www.wired.com/politics/security/commentary/securitymatters/2008/05/blog_securitymatters_0515>

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

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.