

CRYPTO-GRAM
15 agosto 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:

- Promemoria per il prossimo presidente
- La TSA orgogliosa di aver confiscato un oggetto innocuo
- Analisi costi-benefici della sicurezza nazionale
- News
- Hackerare le tessere Mifare
- Information Security e responsabilità
- Responsabilità software e il software libero
- Le news su Schneier/BT Counterpane
- Congratulazioni al nostro milionesimo terrorista!
- Il file system deniable di TrueCrypt
- La vulnerabilità del DNS
- Commenti dei lettori

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

Promemoria per il prossimo presidente

Obama ha un piano per la sicurezza cibernetica.

Si tratta sostanzialmente di quel che ci si aspetterebbe: nominare un consigliere per la sicurezza cibernetica nazionale, investire in educazione matematica e scientifica, stabilire standard per l'infrastruttura critica, investire denaro per il rispetto delle norme, stabilire standard nazionali per la protezione dei dati personali e per la notificazione in

caso di furto di dati, e lavorare congiuntamente all'industria e alle università per sviluppare una serie di tecnologie necessarie.

Potrei fare dei commenti su questo piano, ma per quanto riguarda la sicurezza il diavolo è sempre nei dettagli, e naturalmente in questo momento i dettagli sono scarsi. Ma visto che ha sollevato l'argomento (anche McCain pare che stia "analizzando tali problematiche"), avrei tre suggerimenti di policy per il prossimo presidente, chiunque sarà. Sono troppo dettagliati per essere integrati in discorsi elettorali o in documenti programmatici, ma sono essenziali per migliorare l'information security nella nostra società. Anzi, possono essere applicati in generale anche alla sicurezza nazionale. E sono provvedimenti che soltanto il governo può prendere.

1. Signor presidente, faccia uso del suo immenso potere d'acquisto per migliorare la sicurezza dei prodotti commerciali e dei servizi. Una caratteristica dei prodotti tecnologici è che la maggior parte dei costi viene spesa per lo sviluppo del prodotto, non per la produzione. Prendiamo il software: la prima copia può costare milioni di dollari, ma la seconda è gratuita, per così dire.

Lei deve proteggere i suoi network governativi, sia militari che civili. Deve acquistare computer per tutti i dipendenti del governo. Consolidi quei contratti, e inizi a inserire requisiti di sicurezza specifici nelle richieste d'offerta. Lei ha il potere d'acquisto necessario per fare in modo che i produttori realizzino notevoli migliorie di sicurezza nei prodotti e nei servizi che vendono al governo, e questo sarà un beneficio per tutti perché tali miglioramenti verranno inclusi negli stessi prodotti e servizi che saranno venduti al resto della popolazione. Siamo tutti più protetti se l'information technology è più sicura, malgrado possa essere utilizzata anche dai malviventi.

2. Legiferi sui risultati, non sulle metodologie. Nell'ambito della sicurezza esistono molte aree in cui dovrà approvare delle leggi, aree in cui le esternalità di sicurezza sono tali che il mercato non è in grado di fornire una sicurezza adeguata. Per esempio, le aziende di software che vendono prodotti non sicuri stanno sfruttando un'esternalità analoga a quella delle centrali chimiche che gettano rifiuti nei fiumi. Ma è peggio avere una legge mal congegnata che non avere una legge. Un provvedimento che obbliga le aziende a proteggere le informazioni sensibili è buona cosa; una legge che specifichi le tecnologie che tali aziende dovrebbero utilizzare per proteggere le informazioni non lo è. Stabilire responsabilità sul software per errori e difetti del software è buona cosa, delineare come farlo, no. Legiferi sui risultati che vuole ottenere e metta in atto le sanzioni appropriate; lasci che sia il mercato a occuparsi di come farlo: i mercati sono molto bravi in questo.

3. Investa ampiamente nella ricerca. La ricerca di base è rischiosa perché non sempre ha successo: ecco perché le aziende hanno smesso di finanziarla. Bell Labs non esiste più perché nessuno poteva permettersi di finanziarla dopo lo smembramento di AT&T, ma la causa di fondo era il desiderio di una maggiore efficienza e una redditività nell'immediato che non è del tutto irragionevole in un commercio senza regolamentazioni. La ricerca governativa può essere utilizzata per controbilanciare tutto questo, finanziando una ricerca a lungo termine.

Distribuisca ampiamente i fondi per la ricerca. Ultimamente la maggior parte di essi sono stati reindirizzati attraverso la DARPA per progetti militari a breve termine: non va bene. Impedisca al Congresso, facile agli stanziamenti, di imporre come venga investito il denaro. Lasci che siano la NSF, la NIH e altre agenzie di finanziamento a decidere

come spendere i soldi e non cerchi di fare del micromanagement. E inoltre dia molta libertà ai laboratori nazionali. Certo, alcune ricerche sembreranno sciocche per i profani. Ma non si può prevedere che cosa sarà utile per ottenere qualcos'altro, e se i finanziamenti saranno sottoposti a peer review, i risultati, in media, saranno di molto migliori. Paragonata alle concessioni governative a livello aziendale e ad altre sovvenzioni, è una somma di denaro davvero insignificante.

Per mantenere le nostre capacità di ricerca vive e ricche di entusiasmo occorrono più studenti di matematica e scienza con una preparazione decente a livello di scuola elementare e superiore. In parte la diminuzione d'interesse è dovuta alla percezione secondo cui gli scienziati non diventano ricchi come gli avvocati, i dentisti e gli agenti di borsa; ma anche perché la scienza non viene sufficientemente valorizzata in un paese pieno di creazionisti. Un modo con cui il presidente può dare il proprio contributo è dando fiducia ai consiglieri scientifici, senza annullarne le decisioni per ragioni politiche.

Oh, e cancelli quelle restrizioni post-11 settembre sui visti per gli studenti che stanno obbligando così tanti studenti brillanti a svolgere il proprio lavoro accademico in Canada, Europa e Asia invece che negli Stati Uniti. Tali restrizioni ci danneggeranno nel lungo termine.

Questi sono i tre suggerimenti principali, il resto è nei dettagli. E sono i dettagli a rivestire l'importanza maggiore. Esistono parecchie gravi problematiche di cui lei si dovrà occupare: la privacy delle informazioni, la condivisione dei dati, il data mining, le intercettazioni governative, i database del governo, l'utilizzo dei numeri della previdenza sociale come identificatori, e così via. Non basta raggiungere gli obiettivi di policy generali. Si possono avere le migliori intenzioni e promulgare un'ottima legge, e buttare tutto alle ortiche per due frasi inserite in sordina da qualche lobbista durante la stesura della legge.

La sicurezza è sottile e complessa e, purtroppo, non si presta facilmente ai normali procedimenti legislativi. Lei è abituato a cercare il consenso, ma la sicurezza per consenso funziona raramente. Su Internet, gli standard di sicurezza sono assai peggiori quando vengono sviluppati da un'entità di consenso, e molto migliori quando qualcuno, semplicemente, si mette a elaborarli. Non funziona sempre: molta pessima sicurezza proviene da compagnie che "l'hanno semplicemente implementata", ma da entità di consenso non possono che generarsi standard mediocri. Il punto è che non è possibile ottenere una buona sicurezza senza infastidire qualcuno: l'industria dei broker di informazioni, l'industria delle macchine elettroniche per il voto, le grandi multinazionali delle telecomunicazioni. Con il normale processo legislativo è difficile ottenere una buona sicurezza, ed è per questo che non sono molto ottimista su ciò che lei potrà conseguire a tal proposito.

E se deve nominare un "gran capo" della sicurezza cibernetica, deve affidargli una reale autorità sull'amministrazione del budget. Altrimenti neanche lui sarà in grado di ottenere nulla.

Il piano di Obama:

<http://www.barackobama.com/2008/07/16/remarks_of_senator_barack_obam_95.php>

oppure <<http://tinyurl.com/59ted4>>

<http://www.barackobama.com/2008/07/16/fact_sheet_obamas_new_plan_to.php>

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

McCain:

<<http://www.scmagazineus.com/Cybersecurity-and-the-presidential-campaign/article/112566>>

oppure <<http://tinyurl.com/5h3h75>>

Tecnologie a duplice uso:

<http://www.schneier.com/blog/archives/2008/05/dualuse_technol_1.html>

Buona legislazione:

<<http://www.schneier.com/essay-141.html>>

<http://www.schneier.com/blog/archives/2007/01/information_sec_1.html>

Responsabilità:

<<http://www.schneier.com/essay-025.html>>

<<http://www.schneier.com/essay-116.html>>

Ricerca reindirizzata attraverso la DARPA:

<<http://query.nytimes.com/gst/fullpage.html?res=9F04E1DB113FF931A35757C0A9639C8B63>>

oppure <<http://tinyurl.com/6m6uac>>

Stanzamenti governativi:

<http://www.ostp.gov/pdf/1pger_earmark.pdf>

Problemi legati ai visti studenteschi:

<<http://www7.nationalacademies.org/visas/Statement%20on%20Visa%20Problems.pdf>>

oppure <<http://tinyurl.com/6z7kbo>>

<<http://www.aau.edu/research/Gast.pdf>>

Questo articolo è originariamente apparso su Wired.com:

<http://www.wired.com/politics/security/commentary/securitymatters/2008/08/securitymatters_0807>

oppure <<http://tinyurl.com/5f6dhe>>

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

La TSA orgogliosa di aver confiscato un oggetto innocuo

Che tristezza. La TSA ha confiscato una batteria non perché sia pericolosa, ma perché altri passeggeri potrebbero PENSARE che sia pericolosa. E la TSA è orgogliosa di averlo fatto.

Secondo me, se Kip Hawley potesse commentare sul mio blog, direbbe una cosa di questo tipo: "Non è solo il fatto di vietare le bombe: si tratta di quegli oggetti che sembrano ordigni esplosivi. Tale oggetto assomiglia abbastanza a una bomba da ingannare il resto dei passeggeri, e questo in sé è una minaccia".

Okay, d'accordo. Ma l'uomo della strada non sa come è fatta una bomba, non ne conosce l'aspetto; tutto quel che sa proviene dalla televisione e dai film. E secondo questa regola, tutti i dispositivi elettronici fatti in casa sono da confiscare, perché qualsiasi cosa fatta in casa che abbia dei fili o dei cavi in vista può sembrare una bomba a chi non se ne intende. La regola, quindi, semplicemente non funziona.

E nella realtà di oggi, in cui i passeggeri reagiscono alle minacce, pensate davvero che qualcuno sia in grado di ottenere qualcosa servendosi di un ordigno fasullo?

Ultim'ora: la pagina della TSA è stata aggiornata: ammettono di avere avuto una reazione esagerata.

<http://www.tsa.gov/press/happenings/scot_peekle.shtm>

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

Analisi costi-benefici della sicurezza nazionale

In un eccellente studio di John Mueller, professore di scienze politiche all'Ohio State University, intitolato "The Quixotic Quest for Invulnerability: Assessing the Costs, Benefits, and Probabilities of Protecting the Homeland" [L'irrealistica ricerca dell'invulnerabilità: stima dei costi, benefici e probabilità di proteggere la patria]. Vi sono alcune premesse di buonsenso e conseguenze di policy.

Le premesse:

- "1. Il numero dei potenziali bersagli terroristici è pressoché infinito.
- "2. Le probabilità che uno qualsiasi di tali bersagli verrà attaccato sono essenzialmente nulle.
- "3. Se un bersaglio potenziale ha un certo livello di protezione, l'agile terrorista di solito può prontamente considerare un altro bersaglio.
- "4. Moltissimi bersagli sono 'vulnerabili' in quanto non è difficile danneggiarli, ma invulnerabili in quanto possono essere ricostruiti con relativa rapidità e con spese sostenibili.
- "5. È praticamente impossibile rendere invulnerabile una vasta serie di potenziali obiettivi terroristici, a meno di non chiuderli completamente al pubblico".

Le conseguenze di policy:

- "1. Ogni policy di protezione dovrebbe essere paragonata a un 'caso nullo': non fare nulla, e utilizzare il denaro risparmiato per ricostruire e rimborsare le vittime.
- "2. Lasciare perdere ogni tentativo di immaginare uno specifico elenco di bersagli terroristici.

"3. Considerare gli effetti negativi delle misure di protezione: non solo i costi diretti, ma il disturbo, l'aumento della paura, impatti economici negativi, riduzione delle libertà.

"4. Considerare i costi opportunità e i compromessi delle misure di protezione".

Tutto lo studio merita una lettura approfondita.

<<http://psweb.sbs.ohio-state.edu/faculty/jmueller/ISA2008.pdf>>

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

News

Un impiegato arrabbiato e frustrato tiene in ostaggio la rete informatica di San Francisco, dimostrando che gli insider fidati possono fare parecchi danni.

<<http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/07/14/BAOS11P1M5.DTL&tsp=1>>

oppure <<http://tinyurl.com/69r5x3>>

<http://www.darkreading.com/blog.asp?blog_sectionid=342&f_src=drdaily>

<<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9110520>>

oppure <<http://tinyurl.com/6cse68>>

I fabbri odiano i nerd informatici che imparano a scassinare le serrature.

<<http://www.theglobeandmail.com/servlet/story/RTGAM.20080711.wlpicking11/EmailBNStory/lifeMain>>

oppure <<http://tinyurl.com/5p8jm3>>

<<http://www.crypto.com/papers/safelocks.pdf>>

Divertente sketch radiofonico sul furto d'identità, di Mitchell & Webb.

<<http://www.youtube.com/watch?v=CS9ptA3Ya9E>>

Questo rapporto, "Assessing the risks, costs and benefits of United States aviation security measures" [Stimare i rischi, i costi e i benefici delle misure di sicurezza dell'aeronautica statunitense] di Mark Stewart e John Mueller, è una lettura eccellente. Rinforzare la porta della cabina di pilotaggio è produttivo; gli sky marshal non lo sono. Lo studio finale verrà pubblicato nel Journal of Transportation Security. Non sapevo nemmeno esistesse.

<<http://hdl.handle.net/1959.13/28097>>

Editoriale di opinione del New York Times sul medesimo argomento:

<<http://www.nytimes.com/2008/07/21/opinion/21heifetz.html>>

Chi non sentirebbe un brivido lungo la schiena dopo aver letto questo: "Il Regno Unito è in allarme per un nuovo, micidiale coltello dalla punta esplosiva in grado di congelare gli organi delle vittime". Sì, esiste davvero. È un'arma progettata per chi ha bisogno di uccidere rapidamente animali di grandi dimensioni: squali, orsi, ecc.

<<http://www.dailymail.co.uk/news/article-1035729/Britain-alert-deadly-new-knife-exploding-tip-freezes-victims-organs.html>>

oppure <<http://tinyurl.com/6pr48c>>

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

Non ho idea del perché il Regno Unito sia in allarme per questo. Forse perché i reati in cui viene usato un coltello sono in aumento:

<<http://www.nytimes.com/2008/07/17/world/europe/17knives.html>>

Pare che l'intelligence cinese abbia rubato il BlackBerry di un dipendente di alto livello del governo inglese. Ma la storia non ha senso. Se siete un funzionario dell'intelligence cinese e riuscite a fare in modo che un assistente del Primo Ministro inglese faccia sesso con uno dei vostri agenti, non 'brucereste' immediatamente tale risorsa rubandogli il BlackBerry. Sarebbe stupido. Se mai, clonereste il BlackBerry e glielo restituireste. È possibile che questo sia stato semplicemente un piccolo furto.

<<http://www.timesonline.co.uk/tol/news/politics/article4364353.ece>>

Brillante hacking della Farecard della metropolitana di Washington DC:

<http://www.washingtonpost.com/wp-dyn/content/article/2008/07/18/AR2008071801912_pf.html>

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

In questo articolo sugli autovelox inglesi (in cui si parla anche di un trucco per evitarli che non funziona), c'è questa frase: "Quando i veicoli passano fra il punto di ingresso e di uscita delle telecamere, i numeri di targa vengono registrati digitalmente, sia che il veicolo oltrepassi il limite di velocità, sia che passi a velocità normale". Senza saperne di più, posso garantirvi che tali registrazioni saranno conservate per sempre.

<http://www.theregister.co.uk/2008/07/21/speed_camera_myth/>

Ecco qualcuno nel Regno Unito, il passeggero in una vettura, che mostra il sedere a un autovelox; la sua foto viene pubblicata anche se l'auto non ha oltrepassato il limite di velocità. C'è da chiedersi come sapevano di dover guardare proprio quella fotografia.

<<http://news.bbc.co.uk/1/hi/england/tyne/7378695.stm>>

Stavano confiscando delle creme di protezione solare allo Yankee Stadium come misura antiterrorismo. Questa storia, però, ha un lieto fine. Il giorno successivo alla pubblicazione della vicenda sul New York Post, lo Yankee Stadium ha annullato il divieto. Ora, se solo il Post avesse la stessa influenza sulla sicurezza aeroportuale...

<http://www.nypost.com/seven/07222008/news/regionalnews/sunblockheads_at_the_stadium_120930.htm>

oppure <<http://tinyurl.com/5rl2ns>>

<http://www.schneier.com/blog/archives/2008/06/liquid_ban_gone.html>

<http://www.salon.com/sports/daily/?last_story=/sports/daily/feature/2008/07/23/sun_block/>

oppure <<http://tinyurl.com/67tjn2>>

Adeona è un servizio open source per rintracciare computer portatili.

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

<http://www.pcworld.com/businesscenter/article/148356/new_service_tracks_missing_laptops_for_free.html>

oppure <<http://tinyurl.com/6a8f92>>

Questo estratto proviene da un articolo del Washington Post sui complotti terroristici: "Batiste ha confidato, piuttosto fantasiosamente, di voler far saltare la Sears Tower a Chicago, che si sarebbe poi schiantata su una vicina prigione, liberando detenuti musulmani, i quali sarebbero diventati il nucleo del suo esercito moresco. Con loro, avrebbe costituito la sua propria nazione". 'PIUTTOSTO' fantasiosamente? Sarei curioso

di sapere che cosa il Washington Post considera DAVVERO fantasioso. Un complotto che preveda l'aiuto di Godzilla? Mi sembra chiaro come il Washington Post abbia degli standard molto elevati. Sono stufo di vedere questi idioti presi seriamente. Questo complotto è al di là di fantasioso, è fuori dalla realtà.

<<http://www.washingtonpost.com/wp-dyn/content/article/2008/04/20/AR2008042002227.html>>

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

<http://www.schneier.com/blog/archives/2007/06/portrait_of_the_1.html>

SanDisk ha introdotto schede di memoria di tipo WORM (Write-Once Read-Many) per applicazioni di analisi forense.

<<http://www.sandisk.com/Corporate/PressRoom/PressReleases/PressRelease.aspx?ID=4353>>

oppure <<http://tinyurl.com/5zxeb2>>

Una grande storia di inganni all'epoca della Seconda Guerra Mondiale contenuta nel necrologio di Roger Hall, ex agente dell'OSS (Servizi Segreti). Il libro di Hall sulla sua esperienza nell'OSS, "You're Stepping on My Cloak and Dagger", è lettura obbligatoria.

<http://www.philly.com/inquirer/obituaries/20080723_Roger_Hall_Poked_fun_at_spi es_89.html>

oppure <<http://tinyurl.com/5apy98>>

Un filmato che dimostra come sia facile, con una semplice operazione di ingegneria sociale, introdursi nei locali notturni fingendo di essere il DJ.

<<http://www.5min.com/Video/How-to-Get-Into-Any-Club-14234755>>

Sono stati rubati tremila passaporti britannici vuoti. A me sembra un'operazione dall'interno.

<<http://www.time.com/time/world/article/0,8599,1827501,00.html>>

<<http://www.foxnews.com/story/0,2933,393581,00.html>>

<http://news.sky.com/skynews/Home/Politics/British-Passports-Stolen-After-Van-Hijacked-En-Route-From-Oldham-to-RAF-Northolt/Article/200807415058916?lpos=Politics_1&lid=ARTICLE_15058916_British+Passports+Stolen+After+Van+Hijacked+En+Ro>

oppure <<http://tinyurl.com/6x5g2t>>

Questa è una presentazione video coinvolgente e affascinante, a cura del professor James Duane della Regent University School of Law, che spiega le ragioni per cui, in un contesto penale, non si dovrebbe mai e poi mai parlare con la polizia o con qualsiasi altra entità governativa. Non importa se si è colpevoli o innocenti, se si ha un alibi o meno. È impossibile che qualsiasi cosa diciate possa esservi d'aiuto, mentre è estremamente possibile che anche il dettaglio più innocuo possa danneggiarvi. Vale davvero mezz'ora del vostro tempo.

<<http://video.google.com/videoplay?docid=-4097602514885833865>>

E questo è un filmato dell'agente George Buch del Virginia Beach Police Department, che afferma sostanzialmente che Duane ha ragione.

<<http://video.google.com/videoplay?docid=6014022229458915912&q=&hl=en>>

Vi ricordate quando ho detto che lascio aperta la mia rete wireless domestica? Ecco una buona ragione per non darmi retta. "La polizia indiana, indagando una serie di esplosioni che uccisero 42 persone, ha tracciato un'email in cui si rivendicava l'attentato e ha stabilito che la comunicazione provenisse da un appartamento a

Mumbai. Ordinato un raid a quell'indirizzo, gli agenti di polizia, invece di catturare militanti del gruppo islamico responsabile dell'attacco, ha trovato un gruppo di espatriati americani molto perplessi". Naturalmente i terroristi avrebbero potuto inviare l'email da un luogo qualunque, ma forse è meglio che la polizia non faccia un raid nel VOSTRO appartamento.

<<http://www.guardian.co.uk/world/2008/jul/29/india.terrorism>>

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

Uno dei sospetti autori degli attacchi all'antrace del 2001 si suicida. Materiale affascinante, anche se questa prima storia mi lascia con più domande che risposte.

<<http://www.cnn.com/2008/CRIME/08/01/anthrax.suicide.ap/index.html>>

Il governo degli Stati Uniti ha pubblicato le linee di condotta per il sequestro dei portatili alle frontiere: possono confiscare il vostro portatile dovunque vogliano, per quanto tempo vogliano, e condividere le informazioni con chiunque vogliano.

<<http://www.washingtonpost.com/wp-dyn/content/article/2008/08/01/AR2008080103030.html>>

oppure <<http://tinyurl.com/5w4728>>

<http://www.cbp.gov/linkhandler/cgov/travel/admissability/search_authority.ctt/search_authority.pdf>

oppure <<http://tinyurl.com/5wr7jw>>

<<http://yro.slashdot.org/yro/08/08/01/0958242.shtml>>

<<http://www.schneier.com/essay-217.html>>

Citazione imprecisa delle parole di Schneier:

<http://www.schneier.com/blog/archives/2008/08/schneier_misquo.html>

Ottimo punto di vista sull'estradizione di Gary McKinnon verso gli Stati Uniti.

<<http://www.guardian.co.uk/commentisfree/2008/aug/01/hacking.hitechcrime>>

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

Gli italiani utilizzano soldati per prevenire il crimine. Si tratta soprattutto di una messinscena di sicurezza.

<<http://www.nytimes.com/2008/08/05/world/europe/05italy.html>>

Un portatile contenente delle identità Trusted Traveler è andato perduto; considerato rubato, è stato poi ritrovato.

Laptop with Trusted Traveler identities lost, presumed stolen, and then found.

<http://www.orlandosentinel.com/business/orl-clear0508aug05_0,4458701.story>

oppure <<http://tinyurl.com/6dj35c>>

<<http://cbs5.com/local/tsa.security.clear.2.788083.html>>

<<http://www.tsa.gov/press/releases/2008/0804.shtm>>

<http://www.schneier.com/blog/archives/2007/01/clear_registere.html>

<http://www.schneier.com/blog/archives/2008/06/new_tsa_id_requ.html>

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

<<http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2008/08/05/financial/f102608D05.DTL&tsp=1>>

oppure <<http://tinyurl.com/6fnn8f>>

Il mio articolo su Trusted Traveler:

<<http://www.schneier.com/essay-199.html>>

Molta modulistica della NSA, ottenuta attraverso il Freedom of Information Act:

<<http://www.thememoryhole.org/2008/07/over-400-nsa-forms/>>

Dal blog di Dilbert, una storia assurda sul tema della sicurezza:

<http://dilbert.com/blog/entry/true_story/>

Queste imputazioni a carico della più vasta organizzazione di furti di identità sono state davvero delle grosse novità, ma non credo si tratti di un affare così importante. È ancora molto facile commettere questo genere di reati, ed è tuttora assai difficile catturare i criminali. L'arresto di una banda, anche se di grandi proporzioni, non ci renderà più sicuri.

<<http://www.washingtonpost.com/wp-dyn/content/article/2008/08/05/AR2008080501859.html>>

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

<http://money.cnn.com/2008/08/05/news/companies/card_fraud/?postversion=2008080604>

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

<http://technology.timesonline.co.uk/tol/news/world/us_and_americas/article4468114.ece>

oppure <<http://tinyurl.com/5ldho6>>

<<http://www.ihf.com/articles/ap/2008/08/06/business/NA-US-Retailer-Fraud-Indictment.php>>

oppure <<http://tinyurl.com/6nm8yu>>

<http://www.theregister.co.uk/2008/08/06/id_fraud_hacking_case/>

<http://ap.google.com/article/ALeqM5hIC-7Qgf2_9ytmu5kKBpnEf5XzeQD92D20KG0>

oppure <<http://tinyurl.com/65392t>>

Se vogliamo ridurre i furti di identità, occorre fare in modo che sia più difficile ottenere crediti, effettuare transazioni e in generale svolgere attività finanziarie da remoto.

<http://www.schneier.com/blog/archives/2005/04/mitigating_iden.html>

Il titolo dice tutto: "Passaporto elettronico 'Fakeproof' clonato nel giro di pochi minuti".

<<http://www.timesonline.co.uk/tol/news/uk/crime/article4467106.ece>>

<<http://www.schneier.com/essay-125.html>>

Il DMCA non si applica al governo degli Stati Uniti:

<<http://arstechnica.com/news.ars/post/20080804-air-force-cracks-software-carpet-bombs-dmca.html>>

oppure <<http://tinyurl.com/56rb9w>>

Uccisione casuale su un autobus Greyhound canadese, e la prevedibile reazione esagerata di sicurezza:

<http://www.schneier.com/blog/archives/2008/08/random_killing.html>

The Onion: le Olimpiadi di Pechino sono una trappola?

<http://www.theonion.com/content/video/the_beijing_olympics_are_they_a>

"Amber Alert" come messinscena di sicurezza:

<<http://www.boston.com/bostonglobe/ideas/articles/2008/07/20/abducted/>>

Aggirare la protezione di memoria di Microsoft Vista:

<http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1324395,00.html>

oppure <<http://tinyurl.com/62nqb2>>

<<http://taossa.com/archive/bh08sotirovdowd.pdf>>
<<http://arstechnica.com/news.ars/post/20080811-the-sky-isnt-falling-a-look-at-a-new-vista-security-bypass.html>>
oppure <<http://tinyurl.com/6an5z8>>

Pare che sia cambiata la procedura per viaggiare senza documenti. Ora vengono fatte domande personali sulla propria storia finanziaria.

<<http://philosecurity.org/2008/08/10/flying-without-a-wallet>>

Questo funziona soltanto se avete smarrito i documenti d'identità, non se vi rifiutate di presentarli.

<http://www.schneier.com/blog/archives/2008/06/new_tsa_id_requ.html>

Il Regno Unito ha reso pubblico il National Risk Register (Registro dei rischi per la nazione), precedentemente top secret. Pare che la minaccia più grande per la sicurezza nazionale sia una pandemia di influenza.

<http://www.cabinetoffice.gov.uk/reports/national_risk_register.aspx>

Uno studio interessante sul rischio dell'antrace usata come arma terroristica:

<http://www.stratfor.com/weekly/busting_anthrax_myth>

Non conosco i dettagli, ma rilevare truffe pump and dump sembra un uso eccellente del data mining.

<<http://news.bbc.co.uk/1/hi/technology/7552009.stm>>

<http://news.yahoo.com/s/zd/20080811/tc_zd/230711>

Il data mining funziona al meglio quando esiste un profilo di ricerca ben definito, un numero ragionevole di attacchi all'anno, e un costo contenuto dei falsi allarmi.

<http://www.schneier.com/blog/archives/2006/03/data_mining_for.html>

Esagerare i rischi a cui sono esposti i bambini, e l'efficacia di dar loro un telefono cellulare:

<<http://www.cnn.com/2008/TECH/ptech/08/11/cellphones.kids/index.html>>

La polizia britannica ha sequestrato una copia del gioco di società War on Terror (Guerra al Terrore) perché (ed è una ragione quasi troppo stupida da credersi) la balaclava "potrebbe venire utilizzata per nascondere l'identità di qualcuno o durante l'esecuzione di un atto criminoso". Non si rendono conto le balaclava sono in vendita ovunque nel Regno Unito? O che anche sciarpe, cappucci, fazzoletti e occhiali da sole possono essere utilizzati per nascondere l'identità di qualcuno?

<<http://www.cambridge-news.co.uk/cn%5Fnews%5Fhome/DisplayArticle.asp?ID=338658>>

oppure <<http://tinyurl.com/59ta6r>>

In ogni caso sembra un gioco divertente:

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

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

Hackerare le tessere Mifare

La tessera londinese Oyster è stata craccata, e i dettagli finali saranno resi pubblici a ottobre. NXP Semiconductors, l'azienda derivata dalla Philips che produce il sistema, ha

perso la causa in tribunale per evitare che i ricercatori pubblicassero i risultati. La gente potrà usare queste informazioni per viaggiare gratuitamente sui mezzi di trasporto, ma non sarà di certo una catastrofe. E la pubblicazione di questa grave vulnerabilità, alla lunga, ci renderà tutti più sicuri.

Ecco la storia. Ogni tessera Oyster è provvista di un chip di identificazione a radiofrequenze (RFID) che comunica con i lettori montati sulle barriere di ingresso alle stazioni. Quel chip, chiamato "Mifare Classic", viene impiegato in centinaia di altri sistemi di trasporto (a Boston, Los Angeles, Brisbane, Amsterdam, Taipei, Shanghai, Rio de Janeiro) e anche come pass di accesso in migliaia di aziende, scuole, ospedali ed edifici governativi in Inghilterra e nel resto del mondo.

La sicurezza di Mifare Classic è tremenda. Non sto esagerando: si tratta davvero di sicurezza da giardino d'infanzia. Chiunque abbia un po' di esperienza di sicurezza sarebbe imbarazzato a mettere il proprio nome sul progetto. NXP ha cercato di mascherare quest'imbarazzo mantenendo segreto il design.

Il gruppo che ha craccato Mifare Classic proviene dalla Radboud University Nijmegen nei Paesi Bassi. Hanno dimostrato l'attacco viaggiando gratis in metropolitana e penetrando in un edificio. I loro due studi (uno è già online) saranno pubblicati in occasione di due conferenze quest'autunno.

Il secondo studio è l'oggetto della denuncia di NXP. NXP ha definito "irresponsabile" la divulgazione dell'attacco, ha messo in guardia sul fatto che ciò provocherà "danni incalcolabili", e ha affermato che "comprometterà la sicurezza delle risorse protette da sistemi che incorporano il Mifare IC". La corte olandese non ne ha voluto sapere: "I danni a NXP non provengono dalla pubblicazione dell'articolo ma dalla produzione e vendita di un chip che apparentemente presenta dei difetti".

Esattamente. Più in generale, l'idea che la segretezza sia d'aiuto alla sicurezza è intrinsecamente sbagliata. Ogni qual volta ci imbattiamo in una azienda che dichiara che la segretezza del design è necessaria per la sicurezza (nei documenti di identità, nelle macchine per il voto, nella sicurezza aeroportuale), ciò significa invariabilmente che la sua sicurezza è pessima e che non ha altra scelta se non quella di nasconderla. Qualunque crittografo competente avrebbe progettato la sicurezza di Mifare con un design aperto e pubblico.

La segretezza è fragile. La sicurezza di Mifare era basata sulla convinzione che nessuno avrebbe capito come funzionasse: ecco perché NXP doveva mettere a tacere i ricercatori olandesi. Ma è un modo totalmente sbagliato di procedere. Il reverse-engineering non è difficile. Altri ricercatori avevano già esposto la pessima sicurezza di Mifare. Una compagnia cinese vende persino un chip compatibile. Vi è qualche dubbio che i malviventi non siano già al corrente di questo, o che lo saranno molto presto?

La pubblicazione di questo attacco potrebbe risultare costosa per NXP e i suoi clienti, ma è una buona cosa per la sicurezza in generale. Le aziende progettano la sicurezza al medesimo livello a cui giungono le esigenze dei loro clienti. La sicurezza di NXP era così tremenda perché i clienti non erano in grado di verificare la sicurezza: o non sanno quali domande porre, oppure non sapevano abbastanza per non fidarsi delle risposte di marketing che hanno ricevuto. Questa decisione del tribunale incentiva le aziende a costruire sicurezza correttamente invece di affidarsi a progetti scadenti e alla

segretezza, e le dissuade dal promettere sicurezza basandosi sulle proprie abilità di intimidire i ricercatori.

Non è chiaro l'effetto che avrà questa scoperta sull'azienda di trasporti londinese, Transport for London. La clonazione di una tessera è un lavoro di pochi secondi, e il ladro deve semplicemente sfiorare il possessore di una tessera Oyster legittima. Ma è richiesto un lettore RFID e un programmino; una cosa fattibile per un esperto, ma troppo complicata per il furbacchione medio. È probabile che la polizia arresterà celermente chiunque tenti di vendere tessere clonate a qualsiasi livello. TfL ha promesso di disattivare ogni tessera clonata entro 24 ore, ma ciò danneggerà più la vittima innocente a cui è stata clonata la tessera, che non il ladro.

La vulnerabilità è ancora più grave per quelle compagnie che impiegano Mifare Classic come pass di accesso. Sarebbe molto interessante sapere come NXP presentò loro la sicurezza del sistema.

E mentre questi attacchi riguardano soltanto il chip Mifare Classic, nutro sempre maggiori sospetti su tutta la linea di prodotti. NXP vende un chip più sicuro e ne sta producendo un altro ancora, ma vista la quantità di errori di crittografia basilare commessi da NXP con il chip Mifare Classic, uno non può non domandarsi se le sue versioni "più sicure" lo saranno in maniera adeguata.

Notizie:

<<http://www.guardian.co.uk/technology/2008/jun/26/hitechcrime.oystercards>>
oppure <<http://tinyurl.com/6zby6c>>
<<http://www.ru.nl/ds/research/rfid/>>
<http://technology.timesonline.co.uk/tol/news/tech_and_web/article4184481.ece>
oppure <<http://tinyurl.com/64svrc>>
<<http://www.youtube.com/watch?v=NW3RGbOTLhE>>
<http://news.cnet.com/8301-10784_3-9985886-7.html?hhTest=1>
<<http://www.secureidnews.com/news/2008/07/10/nxp-sues-to-prevent-hackers-from-releasing-mifare-flaws/>>
oppure <<http://tinyurl.com/5brcxr>>
<<http://news.cnet.co.uk/software/0,39029694,49297810,00.htm>>
<<http://www.techradar.com/news/world-of-tech/tfl-responds-to-oyster-hack-runling-428238>>
oppure <<http://tinyurl.com/6cc2ou>>

Uno degli studi:

<<http://www.cs.ru.nl/~flaviog/publications/Attack.MIFARE.pdf>>

La decisione del tribunale olandese:

<http://zoeken.rechtspraak.nl/resultpage.aspx?snelzoeken=true&searchtype=ljn&ljn=BD7578&u_ljn=BD7578>
oppure <<http://tinyurl.com/5a5e3h>>

Segretezza e sicurezza:

<<http://www.schneier.com/crypto-gram-0205.html#1>>

Altre ricerche su Mifare:

<<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9078038>>

oppure <<http://tinyurl.com/6n42p4>>
<<http://www.cs.virginia.edu/~evans/pubs/usenix08/>>
<<http://eprint.iacr.org/2008/166>>
<<http://staff.science.uva.nl/~delaat/sne-2006-2007/p41/Report.pdf>>
<<http://www.translink.nl/media/bijlagen/nieuws/TNO ICT - Security Analysis OV-Chipkaart - public report.pdf>>
oppure <<http://tinyurl.com/66ptjy>>

Il chip cinese compatibile:

<http://www.fmsh.com/english/product_chipcard.php?product=FM11RF32>
<http://www.fmsh.com/english/products/FM11RF32_FS_ENG.pdf>

Questo articolo è originariamente apparso sul Guardian.

<<http://www.guardian.co.uk/technology/2008/aug/07/hacking.security>>

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

Information Security e responsabilità

Un recente studio sull'uso dei browser Internet in tutto il mondo ha scoperto che più della metà (il 52%) degli utenti di Internet Explorer non stanno utilizzando la versione attuale del software. Per altri browser le cifre sono migliori, ma non di molto: il 17% degli utenti di Firefox, il 35% degli utenti di Safari e il 44% degli utenti di Opera stanno utilizzando versioni anteriori del browser.

Questo è particolarmente importante perché i browser sono un vettore sempre più comune per effettuare attacchi internet. Le vecchie versioni dei browser non hanno tutte le patch di sicurezza aggiornate, e sono soggetti ad attacchi che sfruttano vulnerabilità che i produttori hanno già riparato.

I professionisti della sicurezza sono sempre pronti a incolpare gli utenti che non utilizzano l'ultimo update e non installano tutte le patch. "Rimanere aggiornati è essenziale per la sicurezza", dicono, e "se uno non aggiorna il proprio sistema, sua è la colpa se poi subisce un hack". Insomma, è come incolpare la vittima: "Avrebbe dovuto sapere che era pericoloso camminare in quella strada deserta; è colpa sua se lo hanno derubato". È ovvio che la vittima avrebbe potuto, anzi dovuto, prendere ulteriori precauzioni, ma la vera colpa è altrove.

Non è che il patching sia un'operazione tanto semplice. In un contesto aziendale, gli amministratori di sistema fanno fatica a star dietro al flusso infinito di patch software. Ve ne possono tranquillamente essere una dozzina alla settimana, considerando tutti i sistemi operativi e le applicazioni, e troppo spesso una patch crea problemi collaterali. L'Aggiornamento Automatico di Microsoft ha automatizzato il processo, ma è un'eccezione. Il patching rientra in una scelta di priorità, e gli amministratori ne decidono costantemente la priorità tenendo conto di tutte le altre attività che stanno svolgendo.

È il sistema che non funziona. Non esiste nessun'altra industria in cui dei prodotti scadenti vengono venduti a un pubblico che si aspetta problemi in continuazione, e in cui è compito dei consumatori imparare a sistemarli. Se una marca costruttrice di

automobili ha un problema con un modello di auto e pubblica una nota di richiamo, è un evento raro e importante; ed è possibile portare la propria auto per una riparazione gratuita. I computer sono l'unico prodotto di consumo di massa che spinge questo fardello sulle spalle del consumatore, richiedendogli un considerevole livello di esperienza tecnica solo per sopravvivere.

Le cose non dovrebbero andare così. È possibile scrivere del software di qualità. È possibile vendere prodotti software che funzionano bene e non necessitano di continue patch. Il problema è che è costoso e dispendioso in termini di tempo. I produttori di software non lo faranno, ovviamente, perché il mercato non li ricompenserà.

La chiave per sistemare tutto questo sono le responsabilità per il software. I computer sono anche l'unico prodotto di consumo di massa in cui i produttori non accettano responsabilità per i difetti. Il motivo per cui le automobili sono progettate così bene è che i costruttori si assumono le loro responsabilità nel caso facciano qualcosa di sbagliato. Una mancanza di responsabilità per il software è a tutti gli effetti un enorme sussidio governativo dell'industria informatica. Permette alle aziende di realizzare più prodotti più rapidamente, senza troppe preoccupazioni per la sicurezza e la qualità.

La scorsa estate il Science and Technology Committee della House of Lords pubblicò un rapporto sulla "Personal Internet Security" (sicurezza Internet personale). Fui invitato a scrivere un attestato per quel rapporto, e uno dei miei consigli era che i produttori software venissero ritenuti responsabili in caso di errori. Tale consiglio venne incluso nella versione finale del rapporto. Il governo ha respinto i consigli di quel rapporto lo scorso autunno, e l'altra settimana il comitato ha pubblicato un rapporto sulla sua indagine supplementare, che continua a sostenere le responsabilità per il software.

Buon per loro.

Non voglio dare a intendere che la questione delle responsabilità sia semplice, o che la responsabilità per le vulnerabilità di sicurezza debba ricadere interamente sul produttore. Ma i tribunali fanno un ottimo lavoro per quanto riguarda la responsabilità parziale. Una qualsiasi causa legale di responsabilità automobilistica prevede svariate parti potenzialmente responsabili: l'automobile, il conducente, la strada, il tempo meteorologico, probabilmente un altro conducente e un'altra auto, e così via. Analogamente, in un guasto informatico, molte sono le parti parzialmente responsabili: il produttore del software, il produttore del computer, il produttore della rete, l'utente, probabilmente un altro hacker, e così via. Ma non arriveremo mai a questo punto se non partiamo. La responsabilità per il software è la forza di mercato che darà l'incentivo alle aziende per migliorare la qualità del proprio software. E la sicurezza di tutti.

Questo articolo è stato precedentemente pubblicato sul Guardian:

<<http://www.guardian.co.uk/technology/2008/jul/17/internet.security>>

I documenti della House of Lords:

<<http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf>>

oppure <<http://tinyurl.com/27ca43>>

<<http://www.official-documents.gov.uk/document/cm72/7234/7234.pdf>>

<<http://www.publications.parliament.uk/pa/ld200708/ldselect/ldsctech/131/131.pdf>>

oppure <<http://tinyurl.com/58ka8f>>

La responsabilità come metodo per rimediare alle esternalità:

<http://www.schneier.com/blog/archives/2007/01/information_sec_1.html>

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

Responsabilità software e il software libero

Ogni volta che parlo di responsabilità per il software, in molti mi chiedono a proposito del software libero e open source. Se le persone che scrivono software libero, come Password Safe, sono obbligate ad assumersi le responsabilità, semplicemente non potranno farlo, e il software libero finirà con lo sparire.

Non preoccupatevi, non saranno obbligate.

La chiave per capire tutto questo è che tale sorta di responsabilità contrattuale è appunto parte di un contratto, e con il software libero (o con qualsiasi altra cosa libera) non vi è contratto. Il software libero non cadrà sotto un regime di responsabilità perché l'autore del software e l'utente non hanno alcuna relazione commerciale; non sono il venditore e l'acquirente. Mi auguro che i tribunali comprendano questo senza alcuna spinta, ma si potrebbe sempre passare una legge stile Buon Samaritano che protegga le persone che distribuiscono software libero.

Vi potrebbe essere un'industria di aziende che garantiscano responsabilità per il software libero. Se Red Hat, per esempio, vendesse Linux libero, dovrebbe fornire una qualche protezione di responsabilità. Certo, la conseguenza sarebbe un prezzo maggiorato per Linux: quel denaro in più pagherebbe i premi assicurativi. Lo stesso tipo di protezione assicurativa sarebbe a disposizione di aziende che utilizzano altri pacchetti di software libero.

L'industria assicurativa è la chiave per far funzionare tutto ciò. Fortunatamente è un'industria che sa proteggere bene le persone contro le responsabilità. Non c'è ragione di pensare che non sarebbe in grado di farlo anche in questo contesto.

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

Le news su Schneier/BT Counterpane

Schneier intervistato da RU Sirius in aprile:
<<http://www.rusiriusradio.com/2007/04/02/show-98-everything-the-us-government-is-doing-about-security-is-wrong/>>
oppure <<http://tinyurl.com/yuvum2>>
<<http://www.10zenmonkeys.com/2007/04/10/homeland-security-follies/>>

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

Congratulazioni al nostro milionesimo terrorista!

La watch list antiterrorismo statunitense ha raggiunto il milione di nomi. Spero davvero che daremo al nostro milionesimo terrorista un qualche premio.

Chi poteva immaginare che un milione di persone sono terroristi? Perbacco, gli scassinatori negli Stati Uniti sono solo il doppio. E i terroristi sono un numero quindici volte superiore a quello dei piromani.

È o non è tutta un'idiozia, questa?

Alcuni dicono di sistemare quella lista, ma sembra non esserci alcun incentivo a farlo. Sono certo che gli incentivi di carriera non sono allineati in quel modo. Anzi, forse si viene promossi per aver aggiunto delle persone all'elenco. Ma quando si tratta di eliminare qualche nome... se si sbaglia, non importa quanto remota sia tale possibilità, probabilmente sarà la fine della propria carriera. È per questo che nelle società civili abbiamo un sistema giuridico, arbitro imparziale tra forze dell'ordine e accusato. Ma quel sistema sembra non applicarsi qui.

Kafka sarebbe orgoglioso.

D'accordo, non sono un milione di persone. Pare che siano circa 400.000 nomi, solo il 5% degli americani. Non che 400.000 terroristi sia meno assurdo.

"Le agenzie di screening e di polizia si sono imbattute nelle persone della lista (si escludono i falsi positivi) più di 53.000 volte nel periodo fra dicembre 2003 e maggio 2007, secondo un rapporto del Government Accountability Office dello scorso autunno".

Bene, ho una domanda: quanti di quei 53.000 individui sono stati arrestati? E coloro che non sono stati arrestati, perché no? Quanti sono stati eliminati dalla lista dopo essere stati indagati?

<<http://www.aclu.org/privacy/35968prs20080714.html>>
<http://www.fbi.gov/ucr/cius_04/offenses_reported/property_crime/burglary.html>
oppure <<http://tinyurl.com/5wchf5>>
<http://www.fbi.gov/ucr/cius_04/offenses_reported/property_crime/arson.html>
oppure <<http://tinyurl.com/5qs5f7>>
<<http://www.cnn.com/2008/US/07/16/watch.list/index.html>>
<<http://www.propublica.org/article/aclu-million-on-terrorist-watch-list-714>>
oppure <<http://tinyurl.com/5fbsxr>>

Bob Blakely fa due conti:

<<http://notabob.blogspot.com/2008/07/round-up-usual-suspects.html>>

Anche Jon Stewart si fa beffe della lista:

<<http://www.thedailyshow.com/video/index.jhtml?videoId=176627>>

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

Il file system deniable di TrueCrypt

Insieme a Tadayoshi Kohno, Steve Gribble e a tre dei loro studenti all'Università di Washington, ho elaborato un nuovo studio che compromette la funzione di crittografia deniabile di TrueCrypt versione 5.1a. Sostanzialmente, i moderni sistemi operativi si lasciano sfuggire un'incredibile quantità di informazioni, e ciò rende l'essere deniabile un requisito difficile da soddisfare.

Gli studenti hanno svolto la maggior parte del lavoro. Io li ho aiutati con i concetti basilari e ho fornito il modello di minaccia. L'essere deniabile è una funzionalità difficilissima da ottenere.

"Esistono svariati modelli di minaccia contro i quali un DFS (Deniable File System) potrebbe essere potenzialmente sicuro:

"* Singolo accesso. L'aggressore possiede una sola istantanea dell'immagine disco. Un esempio potrebbe essere il sequestro del computer di Alice da parte della polizia.

"* Accesso intermittente. L'aggressore è in possesso di varie istantanee dell'immagine disco, catturate in tempi diversi. Un esempio potrebbe essere dato dalle guardie di frontiera, che fanno una copia del disco di Alice ogni volta che lei lascia il paese o vi rientra.

"* Accesso regolare. L'aggressore possiede molte istantanee dell'immagine disco, prese in brevi intervalli. Un esempio potrebbe essere dato dai servizi segreti, che si introducono quotidianamente nell'appartamento di Alice in sua assenza e fanno una copia del suo disco ogni volta".

Da quando abbiamo elaborato il nostro studio, TrueCrypt ha rilasciato la versione 6.0 del proprio software, e sostiene di aver affrontato molte delle problematiche da noi sollevate. Non abbiamo avuto modo di analizzare la versione 6.0, ma onestamente non ho molta fiducia in proposito.

<<http://www.schneier.com/paper-truecrypt-dfs.html>>
<<http://www.truecrypt.org/docs/?s=hidden-operating-system>>
<<http://www.truecrypt.org/docs/?s=hidden-volume-precautions>>

Articoli in merito:

<http://www.darkreading.com/document.asp?doc_id=159192&WT.svl=news2_1>
<http://www.pcworld.com/businesscenter/article/148513/data_can_leak_from_partialy_encrypted_disks.html>
oppure <<http://tinyurl.com/57ek8x>>
<<http://yro.slashdot.org/article.pl?sid=08/07/17/2043248>>

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

La vulnerabilità del DNS

Malgrado i migliori sforzi della comunità della sicurezza, sono stati resi pubblici i dettagli di una vulnerabilità Internet critica scoperta da Dan Kaminsky circa sei mesi fa. Gli hacker stanno affrettandosi per produrre codice di exploit, e gli operatori di rete che non hanno ancora applicato una patch alla vulnerabilità stanno facendo il possibile per

recuperare il tempo perduto. L'intero pasticcio illustra perfettamente i problemi legati alla ricerca e alla divulgazione di falle come questa.

I dettagli della vulnerabilità non sono importanti, ma in sostanza si tratta di una forma di poisoning della cache DNS. Il sistema DNS è ciò che traduce nomi di dominio comprensibili alle persone, come `www.schneier.com`, in indirizzi IP comprensibili ai computer, come `204.11.246.1`. Esiste un'intera famiglia di vulnerabilità per cui viene fatto credere al sistema DNS sul vostro computer che l'indirizzo IP di `www.sito-maligno.com` sia in realtà l'indirizzo IP di `www.sito-benigno.com` (voi non siete in grado di distinguere le differenze) e questo permette ai criminali di `www.sito-maligno.com` di ingannarvi, facendovi fare qualsiasi cosa, come per esempio comunicare i dati del vostro conto corrente. Kaminsky ha scoperto una variante particolarmente pericolosa di questo tipo di attacco di cache-poisoning.

Inizialmente, l'agenda avrebbe dovuto funzionare così: Kaminsky scoprì la vulnerabilità circa sei mesi fa, e iniziò segretamente a collaborare con i produttori per realizzare una patch. (Il rimedio è piuttosto semplice, ma le sfumature di implementazione sono complesse). Ovviamente questo significava descrivere la vulnerabilità ai vari produttori; altrimenti perché aziende come Microsoft e Cisco avrebbero dovuto credergli? L'8 luglio, Kaminsky ha tenuto una conferenza stampa per annunciare la vulnerabilità, ma non i dettagli, e rivelare che una patch era disponibile presso un lungo elenco di produttori. Tutti avremmo avuto un mese di tempo per applicare la patch, e Kaminsky avrebbe divulgato i dettagli della vulnerabilità alla Black Hat conference il mese prossimo.

Naturalmente, vi è stata una fuga di notizie. Come sia successo non ha importanza, i dettagli avrebbero potuto essere resi pubblici in un miliardo di modi. Troppe persone ne erano a conoscenza perché rimanesse un segreto. Altri che sapevano dell'idea in generale erano troppo brillanti da non mettersi a discutere sui dettagli. Sono anzi piuttosto sorpreso che queste informazioni siano rimaste segrete per così tanto tempo; senza dubbio sono stati rivelati alla comunità underground prima della pubblica divulgazione di qualche giorno fa. E adesso chi aveva deciso di ignorare momentaneamente il problema si sta affrettando ad applicare la patch, mentre la comunità degli hacker si affretta a produrre exploit funzionanti.

Qual è la morale, in questo caso? È facile prendersela con Kaminsky: se non avesse parlato in merito a tale problema, non ci troveremmo in questo pasticcio. Ma è un modo di ragionare sbagliato. Kaminsky ha scoperto la vulnerabilità per caso. Non vi è ragione di credere che fosse il primo a scoprirla, ed è ridicolo credere che sarebbe stato l'ultimo. Ambasciator non porta pena. Il problema è del protocollo DNS: è insicuro.

La vera lezione è che la routine delle patch non funziona, e non funziona da anni. Questo ciclo della scoperta di falle di sicurezza e della corsa a sistemarle prima che i malviventi sfruttino tali vulnerabilità è costoso, inefficiente e incompleto. Dobbiamo progettare la sicurezza nei nostri sistemi fin dal principio. Abbiamo bisogno di certezza, di fiducia, di ingegneri di sicurezza coinvolti nella progettazione di un sistema. Questo processo non potrà prevenire magicamente ogni vulnerabilità, ma è molto più sicuro, ed economico, del ciclo delle patch in cui tutti siamo imprigionati adesso.

Il contributo di un ingegnere della sicurezza al problema è un abito mentale particolare. Egli considera i sistemi da una prospettiva di sicurezza. Non è che scopra tutti gli attacchi possibili prima dei malviventi; più che altro anticipa delle potenziali tipologie di attacco, e prevede delle difese pur non conoscendo i dettagli dei singoli attacchi. Mi

capita di vedere molto spesso una cosa del genere in buoni design crittografici. Si tratta di sovra-ingegnerizzazione che si basa sull'intuizione, ma se l'ingegnere della sicurezza ha un buon intuito, generalmente funziona.

La vulnerabilità di Kaminsky ne è l'esempio perfetto. Anni fa, il crittografo Daniel J. Bernstein esaminò la sicurezza del DNS e decise che la Source Port Randomization era una brillante scelta progettuale. E questa è esattamente la soluzione che è saltata fuori ora sulla scia della scoperta di Kaminsky. Bernstein non aveva scoperto l'attacco di Kaminsky; notò invece una classe generale di attacchi e si rese conto che questa miglioria avrebbe potuto proteggere da tali attacchi. Di conseguenza, il programma DNS da lui scritto nel 2000, djbdns, non ha bisogno della patch: è già immune dall'attacco di Kaminsky.

Ecco come appare un buon design. Non è soltanto il proteggersi da attacchi noti, ma anche il proteggersi da attacchi sconosciuti. Abbiamo bisogno di un maggior numero di applicazioni di questo modo di operare, non solo in Internet ma nelle macchine per il voto, nei documenti di identità, nelle tessere di abbonamento ai trasporti, ovunque. È necessario smettere di dare per scontato che i sistemi siano sicuri fino a che si dimostri la loro insicurezza; occorre invece iniziare a ritenere i sistemi insicuri a meno che non siano progettati in maniera sicura.

Dettagli dell'attacco:

<<http://darkoz.com/?p=15>>

<<http://blog.invisibledenizen.org/2008/07/kaminskys-dns-issue-accidentally-leaked.html>>

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

Notizie:

<<http://news.bbc.co.uk/2/hi/technology/7496735.stm>>

<<http://www.doxpara.com/?p=1162>>

<<http://www.kb.cert.org/vuls/id/800113>>

<<http://www.blackhat.com/html/bh-usa-08/bh-us-08-main.html>>

<<http://it.slashdot.org/it/08/07/21/2212227.shtml>>

<<http://blog.wired.com/27bstroke6/2008/07/details-of-dns.html>>

<<http://addxorrol.blogspot.com/2008/07/on-dans-request-for-no-speculation.html>>

oppure <<http://tinyurl.com/5gp7vm>>

<<http://blog.wired.com/27bstroke6/2008/08/dns-flaw-much-w.html>>

La routine delle patch:

<<http://www.schneier.com/crypto-gram-0103.html#1>>

Certezza:

<<http://www.schneier.com/blog/archives/2007/08/assurance.html>>

L'abito mentale della sicurezza:

<http://www.schneier.com/blog/archives/2008/03/the_security_mi.html>

Il lavoro di Dan Bernstein:

<<http://cr.yip.to/djbdns/forgery.html>>

<<http://cr.yip.to/djbdns/dnscache.html>>

Questo articolo è originariamente apparso su Wired.com:

<http://www.wired.com/politics/security/commentary/securitymatters/2008/07/securitymatters_0723>

oppure <<http://tinyurl.com/5d2kke>>

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

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.