

CRYPTO-GRAM
15 settembre 2007

Scritta da Bruce Schneier
Fondatore e CTO di BT Counterpane

Edizione italiana curata da Communication Valley SpA

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:

- I primi soccorritori
- Gli arbitri di pallacanestro e i singoli punti critici
- Intervista con Mike McConnell, direttore dell'Intelligence USA
- Utenti domestici: un problema di salute pubblica?
- News
- Una reazione esagerata provocata da una minaccia alquanto vaga
- Forse la reazione esagerata più idiota di fronte a una presunta minaccia terroristica
- La sorveglianza automobilistica all'ingrosso arriva a New York
- Le news su Schneier/BT Counterpane
- Il governo USA minaccia ritorsioni contro gli stati che rifiutano il REAL ID
- Studio analitico di informatica forense
- Ottenere cibo gratuito ai fast food drive-in
- Commenti dei lettori

** ** ** * * * * *

I primi soccorritori

Vivo a Minneapolis, quindi il crollo del ponte dell'Interstatale 35W sul fiume Mississippi avvenuto ai primi del mese mi ha colpito da vicino, e se ne è parlato nei notiziari locali e nazionali.

La maggior parte dei primi servizi giornalistici consisteva di storie di interesse umano, incentrate sulle vittime della sciagura e sull'incredibile coraggio dimostrato dai primi soccorritori: i poliziotti, i vigili del fuoco, i paramedici, i subacquei, i soldati della Guardia Nazionale e anche le persone comuni che hanno rischiato la propria vita per salvare quella degli altri (giusto due settimane dopo, tre soccorritori morivano nel tentativo, quasi sicuramente inutile, di salvare sei minatori nello Utah).

Forse l'aspetto più formidabile di queste storie è che non hanno nulla di particolarmente formidabile. A prescindere dalla natura della calamità (uragano, terremoto, attacco terroristico), i primi soccorritori arrivano sulla scena immediatamente dopo.

Ed è proprio per tale ragione che è un delitto che queste persone non possano comunicare fra di loro.

Storicamente i dipartimenti di polizia, i corpi dei vigili del fuoco e i paramedici hanno sempre avuto le proprie distinte attrezzature per le comunicazioni, e di conseguenza quando capita una sciagura che li coinvolge tutti, non possono comunicare fra loro. Un rapporto governativo del 1996, a proposito del primo attentato dinamitardo al World Trade Center del 1993, affermava che "Le procedure di salvataggio delle vittime dell'attentato al World Trade Center, intrappolate fra i piani dell'edificio, furono ostacolate dall'impossibilità degli agenti di polizia di comunicare con i vigili del fuoco che si trovavano giusto al piano superiore".

E tutti sappiamo che la polizia e i vigili del fuoco sono incappati nel medesimo problema l'11 settembre 2001. Si possono leggere i particolari nel libro del vigile del fuoco Dennis Smith e nella deposizione della Commissione sull'11 settembre. Anche il "9/11 Commission Report" [Rapporto della Commissione sull'11/9] ne fa menzione: il Capitolo 9 tratta dei problemi di comunicazione dei primi soccorritori, e i suggerimenti della Commissione per migliorare le comunicazioni di risposta alle emergenze si trovano al Capitolo 12 (pp. 396-397).

In alcune città questa lacuna comunicativa sta cominciando a colmarsi. I fondi della Sicurezza Nazionale hanno raggiunto svariate comunità in tutto il paese. Alcuni li hanno sprecati in improbabili misure di sicurezza come telecamere, robot armati e altre cose che nulla hanno a che vedere con il terrorismo, altri li hanno investiti in risorse per l'interoperabilità delle comunicazioni, come ha fatto lo stato del Minnesota nel 2004.

Ha funzionato. Rich Stanek, sceriffo della Contea di Hennepin, ha dichiarato alla St. Paul Pioneer-Press che sono state salvate molte vite grazie a una pianificazione delle calamità messa a punto e migliorata facendo tesoro dell'esperienza dell'11 settembre:

"Ora abbiamo un sistema di comando unificato dove tutti (la polizia, i vigili del fuoco, l'ufficio dello sceriffo, i medici, i medici legali, i funzionari locali statali e federali) operano sotto un'unica voce", ha affermato Stanek, che sta coordinando i lavori di recupero idrico sul sito del crollo.

“Adesso tutti operiamo sotto gli 800 MHz (di frequenza radio), che fu una delle critiche maggiori dopo l’11 settembre”, ha detto Stanek, “e avere la possibilità di far parlare tra loro 50-60 agenzie è stato semplicemente fantastico”.

Altri non sono stati così fortunati. I primi soccorritori della Louisiana ebbero problemi di comunicazione spaventosi nel 2005, a seguito dell’uragano Katrina. Secondo il National Defense Magazine: “La polizia non era in grado di comunicare con i vigili del fuoco e con le squadre di pronto soccorso. I soccorritori su elicotteri e barche dovevano comunicare a gesti e seguirsi fra loro per poter trovare i superstiti. A volte le forze di polizia e altri primi soccorritori erano isolati da altri compagni che si trovavano nelle vicinanze. I portaordini della Guardia Nazionale correvano da una parte all’altra con messaggi scarabocchiati su fogli di carta, come avveniva durante la Guerra Civile”.

Un rapporto del Congresso sulla preparazione e risposta all’uragano Katrina affermava sostanzialmente le stesse cose.

Nel 2004 la Conference of Mayors USA [Conferenza dei sindaci] pubblicò un rapporto sull’interoperabilità delle comunicazioni. Nel 25% delle 192 città esaminate, la polizia non poté comunicare con il corpo dei vigili del fuoco. Nell’80% delle città le autorità municipali non potevano comunicare con l’FBI, con la FEMA e altre agenzie federali.

L’origine del problema è di ordine economico, e si chiama “problema dell’azione collettiva”. Un’azione collettiva è un’azione che richiede il lavoro coordinato di svariate entità per poter riuscire. Il problema si manifesta quando le esigenze di ciascuna entità divergono da quelle collettive, e non esiste alcun meccanismo che assicuri che tali esigenze individuali siano sacrificate a favore del bisogno collettivo.

Jerry Brito della George Mason University ha dimostrato come questo principio si applichi alle comunicazioni dei primi soccorritori. Ognuna delle oltre 50.000 organizzazioni nazionali di emergency response (dipartimenti di polizia locali, corpi di vigili del fuoco locali, ecc.) acquista il proprio sistema di comunicazioni. Come è lecito aspettarsi, ciascuna entità acquista l’attrezzatura il più possibile adatta alle proprie esigenze. Assicurare l’interoperabilità con le attrezzature di altre organizzazioni va a tutto vantaggio del bene comune, ma sacrificare le proprie specifiche esigenze a favore di tale compatibilità può non essere fra i migliori interessi nell’immediato per ognuna di quelle organizzazioni. Non esiste nessuna direttiva centrale che garantisca l’interoperabilità, e si finisce col non averne affatto.

Questo è un ambito di cui il governo federale può occuparsi e fare qualcosa di buono. Troppo del denaro investito nella difesa contro il terrorismo ha finanziato soluzioni eccessivamente specifiche, efficaci soltanto se i terroristi attaccano un certo bersaglio o fanno uso di una particolare tattica. Il denaro speso per la risposta alle emergenze è diverso: è ugualmente efficace a prescindere dal tipo di complotto terroristico, ed è efficace anche in caso di calamità naturali o che colpiscono l’infrastruttura.

Nessuna sciagura, accidentale o causata volontariamente, è un fenomeno sufficientemente comune da giustificare l’investimento di grandi somme di denaro per la preparazione a un’emergenza specifica. Ma l’investimento di denaro per la preparazione alle catastrofi in generale è un’ottima cosa e sarà sempre ripagata.

Questo articolo è originariamente apparso su Wired.com:

<http://www.wired.com/politics/security/commentary/securitymatters/2007/08/securitymatters_0823>

Nei commenti, i lettori hanno fatto notare che esistono due problemi più grossi del puro aspetto tecnico della questione: l'addestramento e la mancanza di volontà di comunicare. Ciò è verissimo, naturalmente. Fornire delle radiotrasmittenti interoperabili ai primi soccorritori non risolverà automaticamente il problema: devono anche aver voglia di collaborare con altri gruppi.

I soccorritori a Minneapolis:

<<http://www.cnn.com/2007/US/08/02/bridge.responders/>>

<<http://www.ecmpostreview.com/2007/August/8irprt.html>>

<<http://www.cnn.com/2007/US/08/02/bridge.collapse/index.html>>

<<http://michellemalkin.com/2007/08/01/minneapolis-bridge-collapse/>>

<<http://www.cnn.com/2007/US/08/02/bridge.collapse.schoolbus/index.html>>

Sulle morti dei soccorritori nello Utah:

<http://www.boston.com/news/nation/articles/2007/08/17/rescue_worker_killed_at_uh_mine/>

or <<http://tinyurl.com/ywdg6q>>

Il rapporto del 1996:

<http://ntiacsd.ntia.doc.gov/pubsafe/publications/PSWAC_AL.PDF>

Dennis Smith:

<http://www.amazon.com/Report-Ground-Zero-Dennis-Smith/dp/0452283957/ref=pd_bbs_sr_3/104-8159320-0735926?ie=UTF8&s=books&qid=1187284193&sr=8-3>

or <<http://tinyurl.com/223cwb>>

<http://www.9-11commission.gov/hearings/hearing11/smith_statement.pdf>

Il Rapporto della Commissione sull'11 settembre:

<<http://www.gpoaccess.gov/911/index.html>>

Le misure di sicurezza sprecate:

<http://www.schneier.com/blog/archives/2006/03/80_cameras_for.html>

<<http://blog.wired.com/defense/2007/08/armed-robots-so.html>>

<<http://www.cnsnews.com/ViewPolitics.asp?Page=/Politics/archive/200702/POL20070223b.html>>

or <<http://tinyurl.com/2qv5tb>>

<<http://sfgate.com/cgi-bin/article.cgi?f=/c/a/2006/02/19/INGDDH8E311.DTL>>

or <<http://tinyurl.com/yvpw5w>>

Lo stato del Minnesota e l'interoperabilità delle comunicazioni:

<https://www.dps.state.mn.us/comm/press/newPRSystem/viewPR.asp?PR_Num=244>

or <<http://tinyurl.com/2765hp>>

Le parole di Stanek:

Quali tipi di sistemi (IT, finanziario, le partite dell’NBA, ecc.) sono più a rischio di manipolazione? Quelli in cui il cambiamento più piccolo può avere l’impatto più grande, e quelli in cui tale cambiamento può essere effettuato da persone fidate che lavorano all’interno di essi.

Fra tutti i maggiori sport, la pallacanestro è il più vulnerabile alla manipolazione. Vi sono soltanto cinque giocatori in campo per ogni squadra, meno che in altri sport professionistici a squadre; di conseguenza un singolo giocatore può avere un effetto molto maggiore su una partita di pallacanestro rispetto agli altri sport. Stelle del basket come Michael Jordan, Kobe Bryant e LeBron James possono portare un’intera squadra sulle proprie spalle. Nemmeno un grande del baseball come Alex Rodriguez può fare lo stesso.

Dato che i singoli giocatori sono così importanti, un solo arbitro può influenzare una partita di pallacanestro in modo molto più sensibile che in altri sport. Gli arbitri chiamano i falli. In quasi ogni partita avviene un contatto fra i giocatori, e qualsiasi contatto può essere dichiarato falloso. Vengono chiamati “falli tattici” e vengono spesso, ma non sempre, ignorati. Sta agli arbitri decidere quali chiamare.

In maniera ancora più drastica, un arbitro può usare la strategia dei falli per mettere subito nei guai un giocatore fuoriclasse, e fare in modo che l’allenatore lo tenga in panchina per un tempo maggiore nell’arco della partita, se vuole che sia l’altra squadra a prevalere. L’arbitro può stabilire il ritmo del gioco e la quantità di punti segnati a seconda della frequenza con cui chiama i falli. Può decidere di annullare un canestro chiamando un fallo di attacco, oppure dando a una squadra la possibilità di segnare qualche punto in più chiamando un fallo difensivo. Non esiste un replay immediato. Non è prevista una seconda opinione. La parola di un arbitro è legge (vi sono solo tre arbitri) e un arbitro corrotto ha un grande potere di controllo sulla partita.

Non solo gli arbitri di pallacanestro sono singoli punti di rottura: essi sono al tempo stesso persone fidate che lavorano all’interno di un sistema e singoli punti di catastrofica rottura.

Questi generi di vulnerabilità esistono in molti sistemi. Pensate a quel che potrebbe causare alla sicurezza di un aeroporto uno screener della Transportation Security Administration, simpatizzante di un gruppo terroristico. O ai reati di appropriazione indebita di cui potrebbe macchiarsi un CFO criminale. O a quel che potrebbe causare al vostro computer o alla vostra rete un tecnico riparatore disonesto. Stesso dicasi per un giudice (o un agente di polizia, o un funzionario doganale o di frontiera, o un ispettore della sanità, ecc.) corrotto.

Il metodo migliore per scoprire un ‘insider’ corrotto è attraverso l’auditing. I singoli componenti di un sistema che hanno la maggiore influenza sulle prestazioni di quel sistema devono essere monitorati e sottoposti ad auditing, anche se le probabilità di compromissione sono scarse. Avviene dopo il fatto, ma se la probabilità di rilevamento è alta e le sanzioni (multe, detenzione, pubblico disonore) sono severe, è un deterrente piuttosto forte. Naturalmente il contrattacco è prendere di mira il sistema di auditing. Gli hacker cercano continuamente di cancellare i log di audit che contengono prove delle loro intrusioni.

Per l'utente domestico medio, la sicurezza è un problema intrattabile. Microsoft ha fatto sforzi enormi per migliorare la sicurezza del proprio sistema operativo 'out of the box', ma esiste ancora una serie vertiginosa di regole, opzioni e scelte che gli utenti devono seguire e compiere. Come dovrebbero configurare il programma antivirus? Che genere di sistema di backup dovrebbero impiegare? Quali sono le impostazioni migliori per la loro rete wireless? Eccetera eccetera eccetera.

Com'è stato possibile per noi dell'industria informatica creare un prodotto così scadente? Come abbiamo potuto rifilare alla gente un prodotto così difficile da utilizzare in modo sicuro, e che richiede così tanti prodotti aggiuntivi?

Ma è ancora peggio di così. Abbiamo ingannato l'utente medio. Nella nostra corsa a un mercato sempre più in crescita, abbiamo convinto ogni persona ad aver bisogno di un computer. Abbiamo sfornato applicazioni su applicazioni (la messaggeria istantanea, la condivisione peer-to-peer, eBay, Facebook) in modo da rendere i computer più utili e divertenti per l'utente domestico. E allo stesso tempo, li abbiamo resi così difficili da mantenere che soltanto un amministratore di sistema esperto può farlo agevolmente.

E poi ci chiediamo perché gli utenti domestici abbiano così tanti problemi con i loro sistemi bacati, perché non sono in grado di svolgere anche i compiti amministrativi più banali, e perché i loro computer non sono sicuri. Non sono sicuri perché gli utenti domestici non sanno come proteggerli.

Se ho un problema sul lavoro, posso chiamare un intero dipartimento IT. Essi filtrano la mia connessione di rete in modo che lo spam non mi raggiunga, e moltissimi attacchi vengono bloccati ancor prima di raggiungere il mio computer. Mi dicono quali aggiornamenti installare sul mio sistema e quando. E sono a mia disposizione per aiutarmi a ripristinare la macchina nel caso succeda qualcosa di sconveniente al mio sistema. Gli utenti domestici non hanno un supporto tecnico come questo. Se la devono cavare da soli.

Tale problema non è semplicemente destinato a sparire con l'aumentare dell'"intelligenza" dei computer e dell'esperienza degli utenti. La prossima generazione di computer sarà vulnerabile a ogni sorta di attacchi differenti, e la prossima generazione di strumenti di attacco ingannerà gli utenti in nuove altre maniere. Questo braccio di ferro della sicurezza non è destinato a sparire tanto presto, ma sarà combattuto con armi sempre più complesse.

Non si tratta di un problema meramente accademico: è un problema di salute pubblica. Nell'universo iper-connesso di Internet, la sicurezza di ognuno dipende in parte dalla sicurezza di tutti gli altri. Finché vi saranno dei computer non protetti, gli hacker li utilizzeranno per intercettare il traffico di rete, inviare spam, e attaccare altri computer. Siamo tutti più sicuri se tutti quei computer domestici collegati a Internet via ADSL o modem via cavo vengono protetti dagli attacchi. L'unico interrogativo è: qual è il metodo migliore per arrivare a questo?

Mi vengono in mente quelli che dicono "istruite, educate gli utenti". Ci hanno provato, loro? Hanno mai incontrato davvero un utente? Non è realistico pretendere che gli utenti domestici siano responsabili della loro sicurezza. Non ne hanno le conoscenze, e

In Ohio è possibile, per legge, ottenere un elenco dei votanti nell'ordine in cui hanno votato, e un elenco cronologico dei voti. Basta affiancare i due elenchi ed è facile sapere chi ha votato a favore di chi.

<http://news.com.com/E-voting+predicament+Not-so-secret+ballots/2100-1014_3-6203323.html>

or <<http://tinyurl.com/2e63ja>>

<<http://www.freedom-to-tinker.com/?p=1189>>

Mobilio di sicurezza: un comodino "sicuro":

<http://www.jamesmcadam.co.uk/portfolio_html/sb_table.html>

Taser (sì, è il nome dell'azienda e il nome del prodotto) ha ora commercializzato una versione del prodotto per uso personale. Si chiama Taser C2, e incorpora una tecnologia di identificazione interessante. Ogni volta che l'arma viene utilizzata, spara anche dei coriandoli provvisti di codice a barre con un numero seriale, così che sia sempre possibile rintracciare l'arma e, presumibilmente, il proprietario.

<<http://www.taser.com/products/consumers/Pages/C2.aspx>>

Un altro articolo sulla percezione del rischio e sul perché ci si preoccupa delle cose sbagliate.

<http://www.realclearpolitics.com/articles/2007/04/worry_about_the_right_things.html>

or <<http://tinyurl.com/2kgbjz>>

E un grafico eccezionale:

<http://www.nsc.org/lrs/statinfo/odds_dying.jpg>

Non si individueranno i singoli utenti, ma è possibile effettuare un test sulla prevalenza dell'uso di droga in una comunità analizzando le acque di rifiuto. Presumibilmente, se si spinge il campione più a fondo nelle tubature, si può risalire a gruppi di abitazioni o anche alle singole dimore.

<http://www.townhall.com/news/sci-tech/2007/08/21/scientists_drug-test_whole_cities>

or <<http://tinyurl.com/2cuxvb>>

Ecco le cifre della zona del Reno. È stato stimato che, con una popolazione di 38,5 milioni che scarica acque di rifiuto nel Reno fino a Düsseldorf, l'uso di cocaina ammonta a 11 tonnellate metriche all'anno, per un valore di 1,64 miliardi di Euro.

<<http://www.spiegel.de/wissenschaft/mensch/0,1518,383687,00.html>>

Questa chiavetta USB con lucchetto elettronico è un'idea brillante. Solo cinque pulsanti, per un PIN di 10 cifre al massimo; e, quasi certamente, un trillione di possibilità di aggirare la funzione di lucchetto una volta aperto il case. Ma è comunque un'idea nella direzione giusta.

<<http://www.corsair.com/products/padlock.aspx>>

I fusion centers (centri di fusione) sono gestiti dai singoli stati, e ricevono gli aiuti economici dal Dipartimento per la Sicurezza Nazionale. È tutto piuttosto ad hoc, ma il loro obiettivo è quello di 'fondere' l'intelligence federale, statale e locale contro il terrorismo. Ma, guarda caso, non stanno realizzando molta 'fusione' e vengono più comunemente utilizzati per altri scopi.

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

<<http://www.fas.org/sgp/crs/intel/RL34070.pdf>>
<http://www.gcn.com/online/vol1_no1/44629-1.html>

Si è detto e scritto di tutto in merito alla nuova legge tedesca contro gli hacker, che è entrata in vigore in agosto. In sostanza, la legge è talmente malfatta e generica che praticamente nessuno è in grado di rispettarla, né i ricercatori di sicurezza né persino le comuni aziende di software. Se il vostro software viene utilizzato per commettere un reato, potreste essere arrestati.

<http://www.darkreading.com/document.asp?doc_id=132255&WT.svl=news1_5>
<http://www.makezine.com/blog/archive/2007/08/the_hacker_tool_law_in_ef.html?CMP=OTC-0D6B48984890>
or <<http://tinyurl.com/24v8z7>>
<http://www.beskerming.com/commentary/2007/08/12/249/German_Security_Professionals_in_the_Mist>
or <<http://tinyurl.com/2ojhnh>>

In Messico, dei ladri hanno rubato un cane antidroga. Credevo si trattasse di un piano brillante di qualche signore della droga, ma poi il cane è stato ritrovato in un parco, legato a un albero, per cui non so che pensare.

<<http://www.reuters.com/article/oddlyEnoughNews/idUSN2639712520070827>>
<<http://www.reuters.com/article/oddlyEnoughNews/idUSHER84395520070829>>

Questo articolo è una lettura obbligatoria. Tratta della DCSNet (Digital Collection System Network), la rete punta-e-clicca ad alta tecnologia dell'FBI per l'intercettazione domestica. Le informazioni si basano su circa mille pagine di documentazione rilasciata all'EFF sotto il FOIA.

<<http://www.wired.com/politics/security/news/2007/08/wiretap>>
<<http://www.eff.org/flag/061708CKK/>>
<http://www.crypto.com/blog/fbi_wiretaps/>
<<http://www.cs.columbia.edu/~smb/blog/2007-08/2007-08-29.html>>
<<http://yro.slashdot.org/yro/07/08/29/1248212.shtml>>

Immettere password con i movimenti oculari:

<<http://www.stanford.edu/~talg/papers/SOUPS07/Eyepassword-soups07.pdf>>

È stato craccato il filtro antipornografia australiano: il titolone la dice tutta: "Un adolescente cracca in 30 minuti il filtro antipornografia del valore di 84 milioni di dollari australiani" (84 milioni di dollari australiani sono 69,5 milioni di dollari USA: è una bella cifra). Occorre ricordare che qui il problema non è che un ragazzino sveglio possa aggirare il software di censura; è che un ragazzino sveglio, forse questo, forse un altro, possa scrivere uno shareware che permette _a tutti_ di aggirare il software di censura. È lo stesso discorso del DRM: le contromisure tecniche non funzionano.

<<http://www.zdnet.com.au/news/security/soa/Teen-cracks-AU-84-million-porn-filter-in-30-minutes/0,130061744,339281500,00.htm>>
or <<http://tinyurl.com/26n4hq>>

Strana tendenza in ambito di sicurezza fisica:

<http://farm2.static.flickr.com/1372/1234397275_af9e09e8f8.jpg?v=0>
<http://www.schneier.com/blog/archives/2007/08/trends_in_physi_1.html>

Uni-ball sta sfruttando la paura del riciclo degli assegni per vendere le proprie penne. Ammetto che la contraffazione e il riciclo degli assegni siano un problema, ma non mi piace l'utilizzo della paura nella pubblicità.

<<http://www.uniball-na.com/main.taf?p=3,1>>

<http://www.schneier.com/blog/archives/2006/02/check_washing.html>

Microfono-spia laser fai-da-te:

<<http://lifehacker.com/software/diy/build-a-laser-spy-microphone-on-the-cheap-292718.php>>

or <<http://tinyurl.com/3x4huw>>

L'esercito cinese effettua hacking ai danni del Pentagono. Almeno, così si è detto. Onestamente non so che cosa stia succedendo veramente.

<<http://www.ft.com/cms/s/0/9dba9ba2-5a3b-11dc-9bcd-0000779fd2ac.html>>

<<http://arstechnica.com/news/ars/post/20070903-chinese-military-accused-of-hacking-pentagon-computers.html>>

or <<http://tinyurl.com/27oj8z>>

<http://www.theregister.co.uk/2007/09/04/china_hack_pentagon_leak/>

<<http://www.smh.com.au/news/world/china-denies-hacking-pentagon/2007/09/04/1188783237167.html>>

or <<http://tinyurl.com/2mupxv>>

<http://www.salon.com/tech/htww/2007/09/04/chinese_military_hackers/index.html>

or <<http://tinyurl.com/246f9q>>

I dipendenti della NASA sporgono denuncia a causa di background check troppo invadenti:

<<http://www.iht.com/articles/ap/2007/08/30/america/NA-GEN-US-NASA-Background-Checks.php>>

or <<http://tinyurl.com/33eor7>>

<<http://hspd12jpl.org/> (Date un'occhiata al "Forum" se siete davvero interessati.)>

<<http://blog.wired.com/wiredscience/2007/08/jpl-scientists-.html>>

I 'toolkit del crimine cibernetico' fanno notizia:

<<http://news.bbc.co.uk/2/hi/technology/6976308.stm>>

In un certo senso, non vi è nulla di nuovo qui. Da anni esistono in Internet rootkit e kit per costruire virus. Uno 'script kiddie' è appunto per definizione qualcuno che utilizza questi strumenti senza comprenderne l'essenza. L'elemento di novità è il mercato: questi nuovi strumenti non sono fatti per aspiranti hacker, ma per criminali. E con il nuovo mercato arriva anche un business model a scopo di lucro.

La polizia controllerà gli Internet café indiani col pretesto della lotta al terrorismo:

<<http://www.mid-day.com/news/city/2007/august/163165.htm>>

Complotto terroristico sventato in Germania:

<<http://www.nytimes.com/2007/09/07/world/europe/07germany.html>>

<<http://www.washingtonpost.com/wp-dyn/content/article/2007/09/05/AR2007090500209.html>>

or <<http://tinyurl.com/28b7q8>>

<<http://www.timesonline.co.uk/tol/news/world/europe/article2399020.ece>>

<http://www.sfgate.com/cgi-bin/blogs/sfgate/detail?blogid=15&entry_id=20048>

or <<http://tinyurl.com/yohs2m>>
<<http://news.bbc.co.uk/2/hi/europe/6981141.stm>>
<<http://www.msnbc.msn.com/id/20618515/>>

Più leggo a proposito dell'accaduto, più è palese che a catturare questi tizi sia stato un lavoro di intelligence e di investigazione, e non un'operazione di intercettazione all'ingrosso o un qualche programma di data mining.

In India le vacche ottengono documenti di identità con foto:
<http://news.bbc.co.uk/1/hi/world/south_asia/6970305.stm>

Avevo pensato di scrivere in merito al gigantesco attacco distributed-denial-of-service ai danni del governo estone avvenuto in aprile. È stato chiamato la prima guerra cibernetica, anche se non è chiaro se sia stata opera del governo russo. E anche se ho trattato della guerra cibernetica in generale, non mi sono mai occupato degli attacchi contro l'Estonia. Ora non devo neanche farlo. Kevin Poulsen ha scritto un articolo eccellente, che tratta sia la realtà dei fatti sia i sensazionalismi intorno agli attacchi alle reti dell'Estonia, commentando una storia sulla rivista "Wired".

<<http://blog.wired.com/27bstroke6/2007/08/cyber-war-and-e.html>>

La storia su Wired:

<http://www.wired.com/politics/security/magazine/15-09/ff_estonia>

La APEC Conference è stato un evento di grande importanza in Australia, e la sicurezza era agguerrita. Hanno bloccato la maggior parte dell'area di Sydney, implementato delle leggi speciali che per l'occasione garantivano alle forze di polizia ulteriori poteri di perquisizione e ricerca, e hanno persino dato il giorno libero a tutti i lavoratori di Sydney, unicamente per allontanare la gente. Ma i Chasers, un team di comici televisivi, sono riusciti a condurre un finto corteo di automobili con bandiere canadesi oltrepassando tutte le barriere di sicurezza, e nessuno li ha fermati finché non hanno raggiunto l'hotel dove risiedeva il presidente Bush. In una delle vetture si trovava un tizio travestito da Osama Bin Laden.

<<http://www.smh.com.au/news/national/bin-laden-crashes-apec/2007/09/06/1188783415499.html>>

or <<http://tinyurl.com/2vulvr>>

<<http://www.news.com.au/heraldsun/story/0,21985,22376204-5006022,00.html>>

or <<http://tinyurl.com/2ybxdj>>

<<http://www.news.com.au/dailytelegraph/story/0,22049,22377458-5001021,00.html>>

or <<http://tinyurl.com/yqoq98>>

<<http://www.abc.net.au/lateline/content/2007/s2026425.htm>>

<<http://abc.net.au/news/stories/2007/09/07/2027186.htm>>

La stupida sicurezza dell'APEC:

<http://www.smh.com.au/news/national/drop-the-fork-raise-your-hands/2007/09/05/1188783320034.html?s_cid=rss_national>

or <<http://tinyurl.com/yplamf>>

Un ottimo filmato dei Chasers su APEC e la sicurezza, con spezzoni molto divertenti su quel che la gente comune è disposta a fare e ha fatto a loro in nome della sicurezza.

<http://youtube.com/watch?v=JR7I_XlZuck>

Un giudice federale ha abolito il provvedimento del Patriot Act che riguarda la Lettera di Sicurezza Nazionale (National Security Letter, NSL). Il giudice ha immediatamente rinviato la sua decisione, l'appello è ancora in sospeso.

<http://news.yahoo.com/s/ap/20070906/ap_on_re_us/patriot_act_lawsuit>
<<http://www.aclu.org/safefree/nationalsecurityletters/31580prs20070906.html>>
or <<http://tinyurl.com/277p6f>>
<http://www.concurringopinions.com/archives/2007/09/federal_judge_s.html>
or <<http://tinyurl.com/237lmn>>
<<http://www.aclu.org/safefree/nationalsecurityletters/31565lgl20070906.html>>
or <<http://tinyurl.com/yt2crn>>
<http://www.concurringopinions.com/archives/2007/09/some_more_thoug.html>
or <<http://tinyurl.com/2el4ab>>

La no-fly list ha fermato un terrorista vero! Beh, forse. Gerry Adams viene fermato alla frontiera:

<<http://www.guardian.co.uk/travel/2007/aug/24/travelnews.g2>>

Cory Doctorow ha iniziato a curare una rubrica bisettimanale per il "Guardian" sul DRM e l'industria dell'intrattenimento. Finora ha scritto tre pezzi, e si possono trovare qui:

<<http://www.guardian.co.uk/technology/series/digitalwrongs>>

Francobolli elettronici: pessima sicurezza in Germania:

<<http://www.heise-security.co.uk/articles/95341>>

Pochi giorni fa un libro del 1621 sulla crittografia è stato messo all'asta:

<<http://www.liveauctioneers.com/item/4122383/>>

Interessante commento sul rapporto fra le luci e il crimine:

<http://www.schneier.com/blog/archives/2007/09/light_and_crime.html>

A una bambina di quattro anni è stato chiesto di togliersi il cappuccio per delle vaghe ragioni di 'sicurezza':

<http://news.bbc.co.uk/2/hi/uk_news/wales/6983288.stm>

I New England Patriots, una delle due o tre squadre migliori negli ultimi cinque anni, sono stati accusati di aver intercettato i segnali dell'altra squadra mediante una videocamera.

<http://sports.espn.go.com/nfl/columns/story?columnist=clayton_john&id=3014944>

Ricordo di quando la NFL cambiò le regole per permettere un collegamento radio fra il casco del quarterback e la panchina. Una squadra intelligente non solo poteva intercettare le comunicazioni degli avversari, ma deviare il segnale in modo selettivo nei momenti più cruciali. Secondo le regole, se il segnale radio di una squadra non funzionava, l'altra squadra doveva spegnere il proprio, ma non ha molta importanza se si sa che sta per succedere.

È stata condotta con successo un'analisi crittografica del sistema di chiusura auto elettronico KeeLoq:

<<http://redtape.msnbc.com/2007/08/researchers-say.html>>

<<http://www.cosic.esat.kuleuven.be/keeloq/keeloq-rump.pdf>>

Nuove ricerche dimostrano che il firewall nazionale cinese non è poi così efficace:

<<http://news.bbc.co.uk/1/hi/technology/6990842.stm>>

Nuovo sito di vignette sulla sicurezza:
<<http://www.securitycartoon.com/>>

"Say No to Nightmares" [Dite no agli incubi]: un brano originale di Tay Zonday:
<<http://youtube.com/watch?v=CHwKTZ14oFY>>

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

Una reazione esagerata provocata da una minaccia alquanto vaga

Sembra quasi una barzelletta: "Ieri il Dipartimento di Polizia ha organizzato dei checkpoint di sicurezza in Lower Manhattan e ha aumentato il livello di sicurezza dopo aver avuto notizia di una vaga minaccia di attacco radiologico in questa zona".

Inoltre: "La polizia è venuta a conoscenza della minaccia leggendo una parte del sito Web debka.com (secondo Mr Browne, si riteneva che tale sito avesse fonti militari e dell'intelligence israeliana), in cui si diceva che unità operative di Qaeda stavano pianificando la detonazione di un camion riempito di materiale radiologico a New York, Los Angeles o Miami. I funzionari sostengono che il sito Web pubblica rapporti che spesso si rivelano sbagliati, ma che sono occasionalmente fondati".

Occasionalmente fondati? Quale attacco terroristico su suolo statunitense ha previsto in passato?

Andiamo, gente: rifiutate di farvi terrorizzare.

<<http://www.nytimes.com/2007/08/11/nyregion/11threat.html>>
<<http://www.schneier.com/essay-124.html>>

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

Forse la reazione esagerata più idiota di fronte a una presunta minaccia terroristica

È questa la reazione più stupida mai vista prima? "Due persone, avendo versato della farina in un parcheggio per segnare il tracciato per il loro stravagante club podistico, hanno involontariamente causato un allarme bioterroristico e ora sono accusate di reato".

La competizione è feroce, ma credo che ci troviamo di fronte a un vincitore.

Quel che più mi irrita della copertura dei media è che non vi sia il benché minimo accenno al fatto che magari la risposta delle autorità sia stata un tantino fuori dagli schemi.

"Il portavoce del sindaco, Jessica Mayorga, ha detto che la città intende chiedere il risarcimento ai Salchow, che dovranno presentarsi in tribunale il 14 settembre.

“Vi trovate di fronte della polvere collegata da frecce e gesso... non si può mai sapere’, ha continuato, ‘Potrebbe essere l’opera di un terrorista, potrebbe essere qualcosa di più grave. Grazie al cielo non è stato così, ma sono state impiegate molte risorse per stabilirlo”.

Traduzione: abbiamo sbagliato in pieno, e vogliamo che qualcuno paghi per il nostro errore.

<<http://www.msnbc.msn.com/id/20441775/>>

I concorrenti:

<http://www.schneier.com/blog/archives/2007/02/is_everything_a.html>

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

<http://www.schneier.com/blog/archives/2006/08/dropped_ipod_le.html>

<http://www.schneier.com/blog/archives/2007/02/nonterrorist_em.html>

** *** *****

La sorveglianza automobilistica all’ingrosso arriva a New York

New York sta installando un sistema di pedaggio automatico per i veicoli nelle aree più trafficate della metropoli. Viene chiamato congestion pricing (prezzo della mobilità), e si propone di ridurre sia il traffico che l’inquinamento.

Il problema è che mantiene un log di auditing di quali vetture stanno circolando e dove. Il sistema di congestion pricing di Londra viene già utilizzato a scopi antiterroristici, e ora anche per i normali reati. Il sistema di pedaggio automatico E-ZPass, impiegato a New York e altrove, è stato utilizzato sia in processi penali che civili: anche per provare adulterio in una causa di divorzio.

Vi sono ottime ragioni per installare questo sistema, ma temo che sia l’ennesimo strumento di sorveglianza all’ingrosso.

A New York:

<http://www.boston.com/news/nation/articles/2007/08/14/nyc_gets_354_million_for_traffic_toll_plan/>

or <<http://tinyurl.com/2c6tdx>>

A Londra:

<http://www.schneier.com/blog/archives/2007/07/function_creep.html>

<<http://www.timesonline.co.uk/tol/news/uk/crime/article2093557.ece>>

E-ZPass:

<http://www.boston.com/news/nation/articles/2007/09/02/e_zpass_records_make_wa_y_into_criminal_and_civil_trials/>

or <<http://tinyurl.com/24w6hh>>
<<http://www.msnbc.msn.com/id/20216302>>

Sorveglianza all'ingrosso:
<<http://www.schneier.com/essay-147.html>>

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

Le news su Schneier/BT Counterpane

BT Counterpane inaugura un nuovo servizio di rilevamento delle vulnerabilità:
Enhanced Managed Vulnerability Scan Services.
<<http://bt.counterpane.com/pr-20070913.html>>

Un profilo su Schneier è stato pubblicato nella rivista "City Pages".
<<http://www.citypages.com/databank/28/1394/article15776.asp>>

Schneier terrà il keynote alla 29esima edizione della International Conference of Data Protection and Privacy Commissioners, a Montreal, il 25 settembre 2007.
<<http://www.privacyconference2007.gc.ca/>>

Schneier parteciperà all'ACLU Colorado RFID Townhall a Denver il 3 ottobre 2007.

Schneier parteciperà a un evento di beneficenza/presentazione di un libro organizzato dall'EPIC, a Washington DC, il 5 ottobre 2007.
<<http://www.epic.org/events/oct05/>>

Schneier autograferà il suo libro al Gartner Symposium IT Expo a Orlando, Florida, il 10 ottobre 2007.
<<http://www.gartner.com/it/sym/2007/sym17/sym17.jsp>>

Schneier terrà il keynote a Telephony Live! a Dallas, Texas, l'11 ottobre 2007.
<<http://telephonyonline.com/telephonylive/>>

Schneier terrà il keynote a InfoSecurity Mexico, Città del Messico, il 15 ottobre 2007.
<http://ws2.tecnofin.com.mx/p_320.asp?pro=3&sec=2&sub=0>

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

Il governo USA minaccia ritorsioni contro gli stati che rifiutano il REAL ID

REAL ID è il programma del governo USA per imporre normative uniformi sulle patenti di guida statali. È un documento di identità nazionale, almeno da un punto di vista estetico.

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 Counterpane Internet Security, Inc., e membro del comitato consultivo dell'Electronic Privacy Information Center (EPIC). Scrive spesso e tiene conferenze in merito alla sicurezza informatica e alla 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) 2007 - Bruce Schneier.