

CRYPTO-GRAM
15 aprile 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:

Si annuncia il Secondo Concorso "Minaccia da Trama Cinematografica"

Il database antiterrorismo USA

News

JavaScript hijacking

Una banca fraintende il significato dell'autenticazione a due fattori

Le news su Schneier/BT Counterpane

Un fornitore del governo USA inietta software malevolo in computer militari

critici

Il Canile: Brutuslib

Il cyber-attacco

Commenti dei lettori

** ** * * * * * **

Si annuncia il Secondo Concorso "Minaccia da Trama Cinematografica"

Il primo Concorso "Minaccia da Trama Cinematografica" richiedeva di inventare una trama terroristica impressionante e totalmente assurda, ma al tempo stesso plausibile. Tutte le proposte sono state degne di una lettura, ma Tom Grant è stato dichiarato vincitore grazie alla sua idea di far schiantare un aereo pieno di esplosivi contro la diga Grand Coulee.

Quest'anno il concorso è leggermente diverso. Tutti sappiamo ormai che un buon piano per far saltare un aereo provocherà il divieto, o almeno il controllo, di un qualche oggetto o sostanza innocua. Se ci fermiamo un secondo a pensare, è un tipo di risposta decisamente stupida. Abbiamo effettuato controlli su bombe e pistole, e i terroristi hanno utilizzato dei taglierini. Abbiamo vietato taglierini e coltellini, e i terroristi hanno nascosto gli esplosivi nelle scarpe. Abbiamo iniziato a controllare le scarpe, e loro hanno pensato di usare i liquidi. Ora confisciamo i liquidi (anche se gli esperti sono tutti d'accordo nel definire quel piano inverosimile)... E i terroristi si inventeranno qualcos'altro. Non abbiamo speranza di vincere a questo gioco: perché giocarci, allora?

Beh, ci stiamo giocando. E ora potete farlo anche voi. Il vostro obiettivo: inventare una trama terroristica per dirottare o far saltare un aereo utilizzando come componente chiave un comune oggetto che viene solitamente portato a bordo. Tale componente dovrà essere talmente essenziale per la riuscita del piano che la TSA non avrà altra scelta che vietare l'oggetto in questione una volta scoperto il piano terroristico. Voglio vedere una trama impressionante e assurda, ma abbastanza plausibile da venire presa sul serio.

Fate in modo che la TSA proibisca gli orologi da polso. O i computer portatili. O il poliestere. O gli accendini più lunghi di sette centimetri. Insomma, avete capito il concetto.

La vostra proposta verrà giudicata in base all'oggetto scelto (che la TSA non potrà far altro che vietare) e all'ingegnosità della trama. Deve inoltre essere realistica: niente fantascienza, grazie. E il resoconto è essenziale: l'anno scorso le proposte migliori erano anche le più divertenti e piacevoli da leggere.

Come per il primo concorso, presumere un profilo di aggressore simile all'11 settembre: da 20 a 30 individui senza particolari abilità, e un budget di circa 500.000 dollari per acquistare attrezzature, risorse, ecc.

Impostate le vostre "trame cinematografiche", e leggete le altre proposte, sul post nel mio blog.

La giuria sarà composta dal sottoscritto, influenzato dall'eventuale plauso generale nella sezione commenti del blog. Il premio consisterà in una copia autografata di "Beyond Fear" (sia in inglese che in giapponese) e l'adulazione dei vostri pari. E, se mi sarà possibile (l'anno scorso non ho potuto), una telefonata con un vero produttore cinematografico.

La scadenza per la partecipazione è la fine del mese: il 30 aprile.

Lo scopo di questo concorso è un po' di humor surreale, ma mi auguro che serva anche per dimostrare qualcosa. Il terrorismo è una minaccia reale, ma delle misure di sicurezza che ci obbligano a tirare a indovinare quale sarà la prossima mossa dei terroristi non ci rendono affatto più sicuri.

Il post sul blog:

<http://www.schneier.com/blog/archives/2007/04/announcing_seco.html>

La mancanza di plausibilità dell'uso dei liquidi:

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

Il Primo Concorso "Minaccia da Trama Cinematografica":

<http://www.schneier.com/blog/archives/2006/04/announcing_movi.html>

<http://www.schneier.com/blog/archives/2006/06/movieplot_threa_1.html>

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

Il database antiterrorismo USA

Si chiama Terrorist Identities Datamart Environment (TIDE), ed è enorme. Nel 2003 elencava 100.000 nominativi, oggi ve ne sono 435.000. Naturalmente vi sono dei problemi:

"Il TIDE è stato anche causa di preoccupazioni per quanto concerne la segretezza, la privacy ed eventuali errori. Questo elenco per la prima volta riunisce stranieri e cittadini statunitensi in un unico database di intelligence. Non è molto difficile essere inclusi in questo database, e una volta che il nome di qualcuno è presente nell'elenco, è virtualmente impossibile toglierlo. In qualunque momento il processo può portare a terribili vicende kafkiane di nomi scambiati e informazioni non confermate – ha ammesso Travers".

In sostanza l'articolo parla di cose che già conosciamo: l'elenco è pieno di errori, e non esiste un procedimento chiaro e definito per essere inclusi o esclusi dalla lista. Ma la parte più surreale è alla fine, quando interviene Rick Kopel, il direttore del centro:

"Il centro è stato ridicolizzato lo scorso anno quando il programma '60 Minutes' della CBS ha fatto notare che nell'elenco comparivano i nomi di 14 dei 19 direttori dell'11 settembre... cinque anni dopo la loro morte. Kopel ha difeso tale scelta dicendo che 'è un fatto noto che queste persone si serviranno di nomi che ritengono non essere più presenti nel database perché ormai fuori circolazione (sia che appartengano a persone decedute o incarcerate). Non vengono messi a casaccio: ogni nome dell'elenco viene inserito per una ragione precisa' ".

Capito? C'è qualcuno che inserisce nell'elenco nomi sbagliati volontariamente perché crede che i terroristi possano usare degli alias, e li vogliono prendere. Seguendo questo ragionamento, perché allora non mettere nel database l'intero elenco telefonico?

<<http://www.washingtonpost.com/wp-dyn/content/article/2007/03/24/AR2007032400944.html>>
<<http://tinyurl.com/2m6qft>>

oppure

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

News

Articolo del Time Magazine (del novembre scorso) sulla gestione errata del rischio. Molto interessante, e molto simile al mio studio sulla psicologia della sicurezza.

<<http://www.time.com/time/magazine/article/0,9171,1562978-1,00.html>>

È possibile acquistare una Employment Authorization Card statunitense fasulla per 200 dollari.

<http://groups.google.com/group/alt.visa.us.marriage-based/browse_thread/thread/c5eb06ad0ba5f23e/78971a9ce120f1c6#78971a9ce120f1c6> oppure <<http://tinyurl.com/yw6vnn>>

Ecco la tessera vera. Si noti come tutte le caratteristiche di sicurezza della tessera siano falsificate, e molto bene.

<<http://www.immihelp.com/greencard/sample-employment-authorization-card-ead.html>> oppure <<http://tinyurl.com/265od2>>

Un articolo interessante: Neil M. Richards & Daniel J. Solove, "Privacy's Other Path: Recovering the Law of Confidentiality" [Un'alternativa per la privacy: riprendere la legge della riservatezza], 96 Georgetown Law Journal, 2007.

"Terroristi conducenti di autobus" è una minaccia da trama cinematografica che fa leva su due nostre paure: i terroristi e i rischi che corrono i nostri bambini.

<<http://www.foxnews.com/story/0,2933,259168,00.html>>

<http://news.aol.com/topnews/articles/_a/fbi-says-extremists-eye-school-buses/20070316134109990001> oppure <<http://tinyurl.com/2lzfb1>>

<http://www.boingboing.net/2007/03/19/fbi_terrorists_might.html>

Storia interessante di un furto di diamanti basato sull'ingegneria sociale:

<<http://news.independent.co.uk/europe/article2369019.ece>>

L'Ufficio Brevetti degli Stati Uniti sparge FUD per quanto riguarda i download di musica. "Il rapporto, che l'ufficio brevetti ha recentemente inoltrato al Dipartimento di Giustizia degli Stati Uniti, dichiara che le reti peer-to-peer potrebbero manipolare i siti in modo tale che i ragazzini finiscano col violare le leggi sul copyright più frequentemente degli adulti. Secondo il rapporto, ciò renderebbe i ragazzini il bersaglio naturale nella maggioranza delle azioni legali sul copyright e, di conseguenza, farebbe apparire ostili coloro che proteggono il proprio materiale". Ma che è successo? Qualcuno nell'industria dell'intrattenimento ha pagato l'Ufficio Brevetti per scrivere una cosa del genere?

<<http://www.informationweek.com/shared/printableArticle.jhtml?articleID=198000239>

> oppure <<http://tinyurl.com/267zjx>>

<<http://www.uspto.gov/web/offices/com/speeches/07-11.htm>>

Un'altra grande minaccia da trama cinematografica: "Il Personal Car Communicator (PCC) è la connessione intelligente delle chiavi con la vostra Volvo S80, che implementa le soluzioni più all'avanguardia nella comunicazione radio bidirezionale. Quando vi trovate entro il raggio di comunicazione, saprete sempre lo stato della vostra macchina. Aperta o chiusa. Allarme attivato oppure no. Se l'allarme è stato attivato, il sensore di battito cardiaco vi dirà se qualcuno si trova all'interno dell'auto. Il PCC comprende inoltre l'ingresso in auto senza chiavi e la guida senza chiavi".

<<http://www.volvocars.us/models/s80/FeaturesOptions.htm>>

Un comunicato stampa della Ford che spiega questa tecnologia:

<http://media.ford.com/article_display.cfm?article_id=9253>

La polizia di Greater Manchester vuole che tutti la aiutino a scovare terroristi:

<http://www.manchestereveningnews.co.uk/news/s/1000/1000981_help_us_spot_terrorists_police.html> oppure <<http://tinyurl.com/27wuan>>

Questo mi ricorda TIPS, il mal congegnato programma USA che prevedeva che controllori e figure simili, persone che regolarmente entrano in proprietà private, riportassero alla polizia qualsiasi attività sospetta. È un'idea semplicemente idiota: le persone finiranno col segnalarsi fra loro, perché magari il loro cibo ha uno strano odore, o perché parlano una buffa lingua. Il sistema verrà inondato di falsi allarmi, che la polizia dovrà sprecare tempo e risorse per verificare. Questa specie di spionaggio spicciolo approvato dallo stato è qualcosa che ci si aspetterebbe dall'ex Germania Est o dall'ex Unione Sovietica, non dal Regno Unito.

Giusto per fare un paragone, ecco un programma simile che mi piaceva di più.

<http://www.schneier.com/blog/archives/2005/12/truckers_watchi.html>

Controllate la vostra auto da Internet. O, se volete proprio divertirvi, penetrate nel sistema e controllate l'auto di qualcun altro sempre via Internet.

<<http://www.autoblog.com/2007/03/17/you-are-big-brother-control-and-track-your-car-from-the-net/>> oppure <<http://tinyurl.com/29hwcc>>

Vendere e rivendere minuti di traffico telefonico: una nuova interessante variazione della truffa telefonica:

<<http://www.msnbc.msn.com/id/17522658/site/newsweek/>>

Una nuova minaccia a cui non avevo pensato in precedenza: rubare dati dai dischi rigidi delle fotocopiatrici:

<<http://edition.cnn.com/2007/TECH/ptech/03/14/photocopier.risks.ap/index.html>>

oppure <<http://tinyurl.com/25zmdo>>

Google ha nuove regole sulla privacy: ora i dati personali vengono archiviati per due anni invece che all'infinito. È un buon cambiamento, ma non sono sicuro che sia sufficiente. Preferirei davvero che Google cancellasse le informazioni dopo un intervallo più breve.

<http://articles.techrepublic.com.com/2100-1009_11-6167333.html?tag=nl.e019>

oppure <<http://tinyurl.com/2f9I32>>

<<http://www.huffingtonpost.com/huff-wires/20070314/google-privacy>>

Rapporto del CRS sulle macchine della verità. Si notino in special modo le pagine 6-7: la parte dedicata ai falsi positivi.

<<http://www.fas.org/sgp/crs/intel/RL31988.pdf>>

Si veda anche "The Lie Behind the Lie Detector" [La bugia dietro alla macchina della verità]:

<<http://antipolygraph.org/lie-behind-the-lie-detector.pdf>>

La minaccia da trama cinematografica definitiva: gli asteroidi che uccidono. E non ci sono abbastanza fondi per tenerne traccia.

<<http://www.msnbc.msn.com/id/17473059/>>

Tom Kyte, esperto di database Oracle, racconta una storia surreale di un passaggio alla frontiera, dal Canada agli Stati Uniti, e dell'incompetenza del funzionario di dogana:
<<http://tkyte.blogspot.com/2007/03/crossing-border.html>>

Articolo interessante sulla immunità diplomatica come "tessera per uscire gratis di prigione" in Germania.

<<http://www.spiegel.de/international/spiegel/0,1518,468715,00.html>>

"The Straight Dope" sull'immunità diplomatica:

<<http://www.straightdope.com/mailbag/mdiploimmunity.html>>

American Express sta brevettando un sistema per tener traccia delle persone attraverso il RFID. Non so quanto AmEx sia determinata in questo, ma si tratta sicuramente un buon esempio delle possibilità di tale tecnologia.

<<http://www.spychips.com/press-releases/american-express-conference.html>> oppure

<<http://tinyurl.com/3d52je>>

Scandalo di e-voting in Olanda:

<http://www.theregister.co.uk/2007/03/17/foi_dutch/>

Un articolo davvero ottimo su come sbagliamo ad assegnare la colpa nei casi di furto di identità:

<<http://arstechnica.com/news.ars/post/20070314-breaches-of-data-blaming-the-myth.html>> oppure <<http://tinyurl.com/ysfn7e>>

Il governo britannico emette 10.000 passaporti fraudolenti in un anno. Non si tratta di passaporti falsi: sono genuini, ma utilizzati a scopi illeciti. Sono dotati di chip RFID e di ogni misura anti-contraffazione prevista dal governo. Questo è il genere di cosa che dimostra come i vari sforzi per rendere i passaporti più difficili da falsificare non siano la maniera giusta per spendere il denaro destinato alla sicurezza.

<<http://www.guardian.co.uk/terrorism/story/0,,2038442,00.html>>

Questo articolo parla dell'enorme programma di data mining di Singapore. La cosa per me preoccupante è che anche se il Congresso ha interrotto i finanziamenti per il programma, esso è stato sviluppato altrove e ora potrebbe essere rivenduto agli Stati Uniti.

<<http://www.wired.com/politics/onlinerights/news/2007/03/SINGAPORE>>

Le misure di sicurezza incorporate nel nuovo biglietto da 20 sterline inglesi:

<<http://news.bbc.co.uk/1/hi/business/6444003.stm#graphic>>

Come riprendersi dal furto di identità: un elenco specifico per gli Stati Uniti:

<http://www.yourcreditadvisor.com/blog/2007/03/your_identity_h.html>

Sito web di casi giudiziari negli Stati Uniti sul "diritto alla privacy":

<<http://www.law.umkc.edu/faculty/projects/ftrials/conlaw/rightofprivacy.html>> oppure

<<http://tinyurl.com/yeuv3y>>

Nel Regno Unito, i genitori stanno iniziando ad acquistare armature per i loro figli. Un tipo di rischio che sopravvalutiamo costantemente sono i pericoli che possono minacciare i nostri bambini.

<<http://www.timesonline.co.uk/tol/news/uk/article1552956.ece>>

Un grande articolo di The Onion: Al-Qaeda o teenager?

<<http://www.theonion.com/content/node/39374>>

Riflessioni interessanti sui teenager e la valutazione dei rischi, in un articolo sull'auto-
asfissia:

<http://www.schneier.com/blog/archives/2007/03/teenagers_and_r.html>

<<http://www.nytimes.com/2007/03/28/us/28risk.html?ex=1332734400&en=0a99164763a02077&ei=5090&partner=rssuserland&emc=rss>>

oppure

<<http://tinyurl.com/26ot9e>>

La Royal Academy of Engineering (nel Regno Unito) ha appena pubblicato un rapporto, "Dilemmas of Privacy and Surveillance: Challenges of Technological Change" [I dilemmi di privacy e sorveglianza: le sfide del cambiamento tecnologico], dove si discute che la sicurezza e la privacy non sono in opposizione fra loro, e che è possibile ottenere entrambe se affrontiamo la questione con saggezza e razionalità.

<http://www.raeng.org.uk/policy/reports/pdf/dilemmas_of_privacy_and_surveillance_report.pdf> oppure <<http://tinyurl.com/yul7kl>>

<<http://www.raeng.org.uk/news/releases/shownews.htm?NewsID=378>>

<http://www.theregister.co.uk/2007/03/27/security_privacy_study/>

Si leggano almeno i consigli:

<http://www.schneier.com/blog/archives/2007/03/security_plus_p.html>

I Mennoniti stanno pensando di trasferirsi in un altro stato perché non vogliono essere fotografati per la loro patente di guida. Molti stati (tutti?) una volta prevedevano esenzioni di ordine religioso per quanto riguarda l'obbligo di fototessera per tali documenti, ma ora sempre meno stati le garantiscono. A mio avviso il paragrafo più interessante è l'ultimo, in cui viene detto che i cacciatori Amish in Pennsylvania chiedono ai loro vicini non-Amish di acquistare armi per loro, così da aggirare una legge che richiede un documento con foto per acquistare un'arma da fuoco.

<<http://www.msnbc.msn.com/id/17725931/>>

Questo è un articolo datato (del 2000), ma il supplemento in fondo, che descrive come il negozio di elettronica Crazy Eddie abbia commesso una gigantesca frode finanziaria, è assolutamente affascinante.

<<http://www.aicpa.org/pubs/jofa/oct2000/wells.htm>>

Il commento dell'ex CFO di Crazy Eddie:

<http://www.schneier.com/blog/archives/2007/03/crazy_eddie_fin.html#c159443>

oppure <<http://tinyurl.com/2hqk9a>>

Pesci di aprile nell'ambito della sicurezza.

Il mio preferito: Windows Transparency Information Disclosure [Divulgazione di informazioni sulla trasparenza delle finestre]

<<http://www.caughq.org/advisories/CAU-2007-0001.txt>>

Altri:

<<http://www.ndtv.com/convergence/ndtv/story.aspx?id=NEWEN20070007398>>

<<http://www.techliberation.com/archives/042234.php>>

Non so se "Threat Alert" Jesus sia uno scherzo limitato solo al primo aprile, ma è proprio divertente.

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

"2006 Operating System Vulnerability Study" [Studio sulla vulnerabilità dei sistemi operativi - 2006]: lungo ma interessante. Leggete almeno la conclusione.

<<http://www.omninerd.com/2007/03/26/articles/74>>

Durante un'operazione di verifica, un "red team" della TSA è stato in grado di introdurre circa il 90% di armi (non vere, ma riproduzioni) attraverso la sicurezza all'aeroporto di Denver. Non so che cosa sia più importante, se la storia in sé o il fatto che nessuno ne sia sorpreso.

<<http://www.9news.com/news/article.aspx?storyid=67166>>

"Papers, please" [Documenti, prego], un grande studio di Bill Holm del 1990.

<<http://bibdaily.com/pdfs/Papers,%20Please.pdf>>

VBootkit aggira i meccanismi di firma del codice di Windows Vista.

<<http://www.heise-security.co.uk/news/87709>>

Un'affascinante storia narrata in prima persona di un frodatore di carte di credito, estratta da un libro di prossima pubblicazione:

<<http://www.guardian.co.uk/weekend/story/0,,2041537,00.html>>

<<http://www.guardian.co.uk/weekend/story/0,,2041544,00.html>>

Il WEP (Wired Equivalent Privacy) era il protocollo utilizzato per proteggere le reti wireless. È notoriamente insicuro ed è stato sostituito dal WPA (Wi-Fi Protected Access), ma è tuttora in uso. Questo studio mostra come spezzare il WEP a 104 bit in meno di sessanta secondi; a tutt'oggi l'attacco migliore:

<<http://eprint.iacr.org/2007/120.pdf>>

Maggiori informazioni e un'implementazione proof-of-concept:

<<http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw/>>

Una vignetta di Dilbert sui numeri casuali:

<<http://web.archive.org/web/20011027002011/http://dilbert.com/comics/dilbert/archive/images/dilbert2001182781025.gif>> oppure <<http://tinyurl.com/3aav3f>>

E 17 è il numero "più casuale" fra 1 e 20.

<http://scienceblogs.com/cognitivedaily/2007/02/is_17_the_most_random_number.php> oppure <<http://tinyurl.com/358or5>>

<http://scienceblogs.com/cognitivedaily/2007/02/randomness_wrapup.php>

Questo studio, dal numero di febbraio dello "International Journal of Health Geographics" analizza le conseguenze di un attacco nucleare ai danni di parecchie metropoli americane e sostiene che i centri ustioni a livello nazionale sono insufficienti per accogliere tutte le vittime. Viene detto inoltre che sarebbe sufficiente addestrare le persone a fuggire con il vento di traverso per ridurre drasticamente le morti dovute alle precipitazioni radioattive.

<<http://www.ij-healthgeographics.com/content/6/1/5/abstract/>>

<<http://www.ij-healthgeographics.com/content/pdf/1476-072X-6-5.pdf>>
<<http://www.ij-healthgeographics.com/content/6/1/5>>
<<http://www.fas.org/main/content.jsp?formAction=297&contentId=367>>

È da molto ormai che ribadisco che la risposta alle emergenze è un campo in cui si dovrebbero investire denaro e risorse. Questo genere di analisi è al tempo stesso interessante e utile.

Il Dipartimento per la Sicurezza Nazionale vuole chiavi DNSSEC:

<http://www.theregister.co.uk/2007/04/03/dns_master_key_controversy>

La polizia britannica sta pensando di rendere obbligatoria la qualità delle telecamere a circuito chiuso per garantire che le immagini siano all'altezza dei loro standard come prova.

<<http://www.telegraph.co.uk/news/main.jhtml;jsessionid=3E011UQZFRRALQFIQMFSFFOAVCBQ0IV0?xml=/news/2007/03/26/ncctv26.xml>> oppure
<<http://tinyurl.com/22ss5j>>

Per legge, ogni impresa deve controllare i propri clienti mettendoli a confronto con un elenco di "individui con designazione speciale" (Specially Designated Nationals) e ha l'obbligo di non fare affari con nessuno di essi. Naturalmente la lista è piena di nomi errati e molti innocenti finiscono nella rete. E molte imprese decidono che è più semplice respingere potenziali clienti il cui nome è in quell'elenco, creando una sorta di classe di reietti. Questo è il medesimo problema della no-fly list, solo che riguarda un contesto più ampio. E non è un sistema per combattere il terrorismo. Fortunatamente molte imprese non sanno di dover controllare questo elenco, e le persone con nomi simili a sospetti terroristi riescono ancora a condurre una vita sostanzialmente normale. Ma questa tendenza non promette nulla di buono.

<http://www.washingtonpost.com/wp-dyn/content/article/2007/03/26/AR2007032602088_pf.html> oppure
<<http://tinyurl.com/2r6kev>>

La Specifically Designated Nationals List (SDNL):

<<http://www.treas.gov/offices/enforcement/ofac/sdn/index.shtml>>

Anche The Onion interviene su questo argomento:

<http://www.theonion.com/content/infograph/everyday_customers_mistaken>

Analisi interessante la cui conclusione è che non vi è più un gran numero di veri spammer, là fuori:

<<http://www.lightbluetouchpaper.org/2007/04/03/there-arent-that-many-serious-spammers-any-more/>> oppure <<http://tinyurl.com/yrrbyh>>

La polizia tedesca vuole avere il diritto di effettuare hack sui computer:

<http://www.expatica.com/actual/article.asp?subchannel_id=26&story_id=38496>
oppure <<http://tinyurl.com/2fnm2k>>

La sicurezza dei ragazzi di contro alla salute dei ragazzi. Un altro esempio di come sbagliamo a valutare i rischi.

<<http://www.post-gazette.com/pg/07093/774604-51.stm>>
<http://www.boingboing.net/2007/03/04/no_child_left_inside.html>

Ottimo commento sul blog:

<http://www.schneier.com/blog/archives/2007/04/childhood_safet.html#c162565>
oppure <<http://tinyurl.com/24ljeo>>

Questo estratto da un comunicato stampa è fantastico: "Il computer era protetto da due livelli di sicurezza, un identificatore utente e una password multicarattere alfanumerica". Sveglia! Avere un nome utente e una password (anche se sono entrambi segreti) non conta come due fattori, due livelli, o due qualsiasi altre cose. È necessario avere DUE DIVERSI sistemi di autenticazione: una password e un dato biometrico, una password e un token, ecc. Io non affiderei il mio denaro alla New Horizons Community Credit Union.

<http://www.ncua.gov/news/press_releases/2007/MR07-0411.htm>

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

JavaScript hijacking

Il JavaScript hijacking (lett. "dirottamento di JavaScript") è un nuovo tipo di attacco di intercettazione mirato alle applicazioni Web in stile Ajax. Sono piuttosto sicuro che si tratti del primo genere di attacco che prende specificamente di mira il codice Ajax. Tale attacco è reso possibile dal fatto che i browser web non proteggono il JavaScript nello stesso modo con cui proteggono il codice HTML; se un'applicazione Web trasferisce dati sensibili mediante messaggi scritti in JavaScript, tali messaggi in alcuni casi possono essere letti da un aggressore.

Gli autori dello studio dimostrano che molti framework di programmazione Ajax assai diffusi non fanno nulla per evitare il JavaScript hijacking. Alcuni addirittura _obbligano_ un programmatore a creare un server vulnerabile affinché possano funzionare.

Come per molte altre di queste tipologie di vulnerabilità, è facile impedire la classe di attacchi. In molti casi sono sufficienti alcune righe di codice in più. E come per molti altri problemi di sicurezza del software, i programmatori devono comprendere le implicazioni di sicurezza del loro lavoro, così da poter attenuare i rischi che affrontano. Ma suppongo che il problema del JavaScript hijacking non verrà risolto tanto facilmente, perché molti programmatori non comprendono le implicazioni di sicurezza del loro lavoro, e non impediranno gli attacchi.

Lo studio:

<http://www.fortifysoftware.com/servlet/downloads/public/JavaScript_Hijacking.pdf>
oppure <<http://tinyurl.com/28nzje>>

Uno dei co-autori dello studio risponde a molti dei commenti apparsi sul mio blog:

<http://www.schneier.com/blog/archives/2007/04/javascript_hija_1.html#c160667>
oppure <<http://tinyurl.com/yqaoz5>>

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

Una banca fraintende il significato dell'autenticazione a due fattori

Dal comunicato stampa: "Il computer era protetto da due livelli di sicurezza, un identificatore utente e una password multicarattere alfanumerica".

Sveglia! Avere un nome utente e una password (anche se sono entrambi segreti) non conta come due fattori, due livelli, o due qualsiasi altre cose. È necessario avere DUE DIVERSI sistemi di autenticazione: una password e un dato biometrico, una password e un token, ecc.

Io non affiderei il mio denaro alla New Horizons Community Credit Union.
<http://www.ncua.gov/news/press_releases/2007/MR07-0411.htm>

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

Le news su Schneier/BT Counterpane

Lo scorso mese ho accettato il mio EFF Pioneer Award. Sono disponibili l'audio e il video del mio discorso.

<http://www.archive.org/details/Bruce_Schneier_EFF_Pioneer_Awards_2007>
<<http://stage6.divx.com/EFF/video/1179205/Bruce-Schneier-EFF-Acceptance-Speech>>
oppure <<http://tinyurl.com/ytdskp>>

Mi fa molto piacere ricevere il premio, e sono davvero colpito da queste parole di Cory Doctorow: "La tecnologia non arriverà mai a ottenere ciò che possono conseguire i valori fondamentali di una società democratica. Possiamo cambiare il mondo con il potere delle idee. Sfido chiunque a leggere gli splendidi libri di Bruce e a non cambiare la propria visione del mondo".

<http://blog.wired.com/business/2007/03/words_of_wisdom.html>

T-shirt di Bruce Schneier (io non ho nulla a che vedere con tutto questo):

<<http://geekz.co.uk/shop/store/show/schneier-tshirt>>
<http://www.goodstorm.com/item/pbutler/what_would_bruce_schneier_do>
<http://www.goodstorm.com/item/pbutler/schneier_mosaic>

Adesivi:

<<http://geekz.co.uk/shop/store/show/schneier-sticker-0>>

Un ennesimo capitolo della mia "vita surreale".

RU Sirius mi ha intervistato per il suo podcast.

<<http://www.rusiriusradio.com/2007/04/02/show-98-everything-the-us-government-is-doing-about-security-is-wrong/>> oppure <<http://tinyurl.com/yuvum2>>

eWeek mi ha messo al 40esimo posto della classifica delle cento persone più influenti nell'ambito dell'IT.

<http://www.eweek.com/slideshow_viewer/0,1205,l=%26s=26744%26a=203626%26po=12,00.asp> oppure <<http://tinyurl.com/yu2oqy>>

IT.com mi ha inserito nella classifica delle 59 persone più influenti nell'ambito della sicurezza IT.

<<http://www.itsecurity.com/features/top-59-influencers-itsecurity-031407/>> oppure
<<http://tinyurl.com/yroh8b>>

Articoli su Schneier dall'India:

<<http://www.schneier.com/news-031.html>>

<<http://economictimes.indiatimes.com/articleshow/1775503.cms>>

Wired ha pubblicato un estratto del mio studio "Psychology of Security" [La psicologia della sicurezza]:

<http://www.wired.com/politics/security/commentary/securitymatters/2007/03/SECURITY_MATTERS0322> oppure <<http://tinyurl.com/2dez23>>

Schneier interverrà al Electronic Transactions Association Annual Meeting and Conference a Las Vegas il 19 aprile.

<http://www.electran.org/events/annual_meeting.asp>

Schneier è l'esperto ospite d'onore al Penguicon a Troy, Minnesota, il 20-22 aprile.

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

Schneier interverrà alla conferenza Computers, Freedom and Privacy a Montreal il 4 maggio.

<<http://www.cfp2007.org/>>

Schneier terrà un discorso a nome dell'ACLU a Iowa City, Iowa, il 5 maggio.

*** **

Un fornitore del governo USA introduce software malevolo in computer militari critici

Questa è semplicemente una storia allucinante. In sostanza, un fornitore con una autorizzazione di sicurezza top secret è stato in grado di introdurre codice malevolo e di sabotare dei computer impiegati per il tracciamento di sottomarini della Marina Militare.

Certo, è stato seccante dover trovare e risolvere il problema, ma aspettate un attimo: com'è possibile che un singolo imbecille frustrato possa danneggiare un sistema di armamenti che vale molti miliardi di dollari? Perché non vengono implementati dei sistemi di sicurezza per evitare una cosa del genere? Scommetto quel che volete che non vi è stato il benché minimo controllo o verifica su chi abbia inserito che tipo di codice e dove lo abbia inserito. Scommetto che se questo tizio fosse stato solo un po' più sveglio avrebbe potuto causare molti più danni senza venire mai preso.

Uno dei metodi per gestire il problema degli individui fidati è quello di assicurarsi che siano degni di fiducia. Il processo di autorizzazione dovrebbe appunto prendersi cura di ciò. Ma dato l'enorme danno che una sola persona può fare in questo contesto, è assolutamente necessario aggiungere un secondo meccanismo di sicurezza: limitare il livello di fiducia che è possibile assegnare a ogni individuo. Un sistema decente di revisione del codice, di traccia dei cambiamenti, ridurrebbe di gran lunga il rischio che accada una cosa del genere.

Infine scommetto qualsiasi cosa che esiste maggior sicurezza intorno al codice essenziale di Microsoft che non a quello del sistema militare degli Stati Uniti.

<<http://content.hamptonroads.com/story.cfm?story=122352&ran=199274>>

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

Il Canile: Brutuslib

Siamo nel 2007 e non posso credere che le persone stiano usando ancora degli algoritmi crittografici fatti in casa. Questo sembra molto facile da compromettere.

<<http://www.yan.cz/brutuslib/hdiw.php?lang=en>>

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

Il cyber-attacco

Il mese scorso, il Generale dei Marines James Cartwright ha detto al House Armed Services Committee che la miglior difesa cibernetica è un buon attacco.

Secondo quanto riportato dal "Federal Computer Week", Cartwright ha detto: "La storia ci insegna che un atteggiamento puramente difensivo è causa di rischi significativi", e che "se applichiamo il principio dello stato di guerra anche al cyberspazio così come viene applicato per mare, aria e terra, possiamo comprendere come giovi maggiormente alla difesa del paese investire in risorse in grado di portare l'attacco contro i nostri nemici quando sia necessario, in modo da impedire azioni nocive ai nostri interessi".

Il generale non è il solo a pensarla così. Nel 2003 l'industria dell'intrattenimento ha cercato di far approvare una legge che le garantisse il diritto di attaccare qualsiasi computer sospettato di distribuire materiale protetto da copyright. E probabilmente a tutti gli amministratori di sistema nel mondo piacerebbe contrattaccare e colpire quelle macchine che stanno attaccando ciecamente e ripetutamente le loro reti.

Naturalmente quel che dice il generale è giusto. Ma il suo ragionamento illustra perfettamente il perché stato di pace e stato di guerra siano due cose ben diverse, e perché i generali non sarebbero ottimi comandanti delle forze di polizia.

Una politica di cyber-sicurezza che ammette sia la deterrenza attiva sia la ritorsione, senza alcuna determinazione giudiziaria di atto illecito, è indubbiamente una soluzione attraente, ma è sbagliata; se non altro perché ignora il confine tra guerra, in cui alle parti coinvolte è permesso stabilire quando sia necessario contrattaccare, e reato, nel cui ambito solo terze parti imparziali (giudici e giurie) possono imporre una pena.

Nello stato di guerra il concetto di contrattacco è estremamente potente. Attaccare il nemico, le sue postazioni, le sue linee di alimentazione, le sue fabbriche, la sua infrastruttura, è una tattica militare antichissima. Ma in tempo di pace tutto questo si chiama vendetta, e viene considerato pericoloso. Chiunque sia accusato di un reato merita un giusto processo. L'accusato ha il diritto di difendersi, di affrontare il suo accusatore, di essere rappresentato da un avvocato e di essere considerato innocente fino a prova contraria.

Sia i contrattacchi di vigilanza che gli attacchi preventivi sfidano apertamente questi diritti. Vanno a punire persone che non sono state provate colpevoli. Il concetto è il medesimo sia che si tratti di una folla inferocita che si scaglia contro un sospettato, sia che si tratti della MPAA che disabilita il computer di qualcuno che si ritiene abbia copiato illegalmente un film, sia che si tratti di un funzionario di sicurezza di un'azienda che lancia un attacco denial-of-service contro qualcuno che crede stia prendendo di mira la rete aziendale.

In tutti questi casi, l'aggressore potrebbe avere torto. È accaduto con i linciaggi, e su Internet è ancora più difficile stabilire chi vi sta attaccando. Solo perché il mio computer sembra essere la fonte di un attacco non significa che lo sia davvero. E anche se fosse, potrebbe trattarsi di una macchina zombie controllata da un altro computer; anch'io potrei essere una vittima. L'obiettivo del sistema legislativo di un governo è la giustizia; lo scopo di un vigilante è il vantaggio, l'utilità, l'opportunità.

Comprendo le frustrazioni del Generale Cartwright, come comprendo quelle dell'industria dell'intrattenimento e degli amministratori di sistema sparsi per il mondo. La giustizia nel cyberspazio può essere difficile. Può essere arduo capire chi ci sta attaccando, e può volerci molto tempo prima di poter fermare questa o queste persone. Può risultare ancor più arduo portare delle prove di fronte a un tribunale. La natura internazionale di molti attacchi non fa che aggravare i problemi. Un numero sempre maggiore di criminali cibernetici saltellano di giurisdizione in giurisdizione, attaccando da paesi che non possiedono delle leggi efficaci contro i reati informatici, che hanno forze di polizia facilmente corruttibili e nessun trattato di estradizione.

La vendetta, la ritorsione, sono soluzioni molto semplici e attraenti, e considerare l'intera questione come fosse un problema militare è più facile che lavorare all'interno del sistema legale.

Ma ciò non la rende giusta. Nel 1789, la Dichiarazione dei Diritti dell'Uomo e del Cittadino dichiarava: "Nessun uomo può essere accusato, arrestato o detenuto se non nei casi determinati dalla Legge, e secondo le forme da essa prescritte. Quelli che procurano, spediscono, eseguono o fanno eseguire degli ordini arbitrari, devono essere puniti".

Mi fa piacere che il Generale Cartwright pensi a una guerra cibernetica di attacco e contrattacco: è così che pensano i generali. Sono persino d'accordo con Richard Clarke, che minaccia una reazione di tipo militare in caso di attacco cibernetico da parte di un paese straniero o di un'organizzazione terroristica. Ma in mancanza di un atto di guerra, siamo molto più al sicuro con un sistema legale che rispetta i nostri diritti.

<<http://www.fcw.com/article98016-03-22-07-Web>>

Permettere all'industria dell'intrattenimento di contrattaccare mediante hacking:
<<http://www.politechbot.com/docs/berman.coble.p2p.final.072502.pdf>>
<<http://www.freedom-to-tinker.com/?cat=6>>

I commenti di Clarke:
<<http://www.usatoday.com/tech/news/2002/02/14/cyberterrorism.htm>>

Questo articolo è originariamente apparso su Wired.
<http://www.wired.com/politics/security/commentary/securitymatters/2007/04/securitymatter_0405> oppure <<http://tinyurl.com/2dkpcc>>

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

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 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.