

CRYPTO-GRAM
15 settembre 2004

Scritta da Bruce Schneier
Fondatore e CTO di Counterpane Internet Security, Inc.

Edizione italiana curata da Communication Valley SpA

E-mail: schneier@counterpane.com

Web: < <http://www.schneier.com> > oppure < <http://www.counterpane.com> >

CRYPTO-GRAM è una newsletter mensile gratuita che offre riassunti, analisi, approfondimenti, e commenti sulla sicurezza (informatica e in generale) e sulla crittografia.

Crypto- Gram in versione originale è anche consultabile in formato RSS:
< <http://www.schneier.com/crypto-gram-rss.xml> >

** **

In questo numero:

“Beyond Fear”: primo anniversario
La sicurezza alle Olimpiadi
Crittanalisi di MD5 e SHA
Le ristampe di Crypto- Gram
Il programma Trusted Traveler
Note di sicurezza da ogni dove: la sicurezza dei musei
News
Le News di Counterpane
Spoofing e cellulari finlandesi
La cosiddetta “No- Fly List”
Commenti dei lettori

** **

Beyond Fear: primo anniversario

Il mio libro più recente, “Beyond Fear”, compie un anno questo mese.

L'ho scritto per spiegare come funziona la sicurezza. L'idea era quella di prendere l'approccio metodico alla sicurezza tipicamente sviluppato nell'universo dell'informatica ed applicarlo a tutti gli altri tipi di sicurezza: personale, aziendale, nazionale. Nel libro propongo di vedere la sicurezza come un sistema, e tutto ciò che esso implica. Parlo del concetto di anello debole di una catena, e di ciò che significa per quanto concerne l'efficacia della sicurezza. Parlo di strategie di sicurezza diversificate (barriere, autenticazione, divisione in compartimenti, persone “fidate”, contrattacco, ecc.) che sono state sviluppate nei secoli, e di come possano essere applicate per tentare di risolvere i problemi di sicurezza odierni.

Ho molte cose da dire sulla sicurezza nazionale e sul terrorismo, concetti e analisi che cercano di innestare un po' di buonsenso in quel che è ormai diventato un dibattito intriso di politica.

Il libro ha avuto successo, ma non ha mai raggiunto la massima visibilità. Le recensioni (anche quelle presenti in pubblicazioni che non trattano di informatica) sono state unanimemente

cannoniere e sommozzatori che pattugliavano i porti. Ma la sicurezza dietro le quinte è stata ancora maggiore. Secondo i comunicati stampa delle Olimpiadi era presente un sistema di 1250 telecamere di sorveglianza ad alta risoluzione e agli infrarossi montate su pali di cemento. Altri dati di sorveglianza venivano raccolti da sensori presenti su 12 motovedette, 4000 veicoli, 9 elicotteri, 4 centri di comando mobili e un dirigibile. Non si trattava solo di immagini; vari microfoni registravano le conversazioni, un software di riconoscimento vocale le trasformava in testo scritto e un software sofisticato di ricerca e riconoscimento di schemi si metteva alla ricerca di frasi, codici, schemi sospetti. La sicurezza alle Olimpiadi ha impiegato in totale 70.000 persone, circa sette per atleta o una per ogni 76 spettatori.

Il governo greco, secondo quanto è stato riferito, ha speso un miliardo e mezzo di dollari in sicurezza durante le Olimpiadi. Ma, a parte statistiche e spiegamenti di forze, questi soldi sono stati ben spesi? Sotto molti aspetti, la sicurezza alle Olimpiadi può essere vista come un'anteprima di quel che potrebbe essere in futuro vivere negli USA. Se le Olimpiadi devono essere un banco di prova per la sicurezza, allora vale la pena di esaminare in che misura tale sicurezza ha davvero funzionato.

Purtroppo non è cosa semplice. Abbiamo a disposizione del materiale per la stampa, ma i dettagli sulla sicurezza rimangono segreti. Sappiamo, ad esempio, che SAIC ha sviluppato l'imponente sistema elettronico di sorveglianza, ma dobbiamo fidarci di quel ci dicono loro per quanto riguarda l'efficacia. Ora, SAIC è un nome di tutto rispetto: erano uno dei fornitori che costruirono il sistema di intercettazione elettronico ECHELON per la NSA, e presumibilmente avranno qualche asso nella manica. Ma quanto bene rileva conversazioni oppure oggetti sospetti, e quanto spesso produce falsi allarmi? Non ne abbiamo idea,

Ma anche se non possiamo esaminare i funzionamenti interni della sicurezza delle Olimpiadi, abbiamo alcuni fugaci esempi della sicurezza in azione.

Un reporter del Sunday Mirror ha raccontato di ogni genere di problemi con la sicurezza. Dapprima ha ottenuto un posto come autista da un appaltatore inglese. Non ha prodotto referenze di alcun tipo, non ha sostenuto alcun colloquio né alcun background check, e gli è stato da subito garantito l'accesso allo stadio principale. Ha notato che il suo furgone non è mai stato sottoposto a un'attenta perquisizione, e che lui avrebbe potuto introdurre nello stadio qualsiasi cosa. È stato in grado di posizionare tre pacchi pensati per assomigliare a bombe, tutti passati inosservati durante i controlli di sicurezza. Ed è riuscito a stare a meno di 20 metri da dozzine di capi di stato durante le cerimonie d'apertura.

In un incidente isolato, un uomo con indosso un tutù e scarpe da clown è riuscito a tuffarsi da un trampolino e nuotare per diversi minuti prima di essere tirato fuori dagli ufficiali della sicurezza. Ha affermato di voler mandare un messaggio a sua moglie, ma il nome di un sito web di giochi d'azzardo online stampato sul suo petto faceva presumere motivazioni più commerciali.

E l'ultimo giorno delle Olimpiadi, un corridore brasiliano che stava conducendo la maratona maschile, a pochi chilometri dal traguardo è stato spinto fuori dal percorso di gara da un intruso irlandese in costume. Alla fine il corridore è arrivato terzo; il suo distacco stava diminuendo prima dell'incidente, ma non possiamo dire quanto gli sarebbe costato.

Questi tre incidenti hanno solo valore anedddotico, ma dimostrano un fatto importante per quanto riguarda la sicurezza in questo genere di eventi: è piuttosto impossibile fermare un singolo individuo intenzionato a combinare guai. Non importa quante telecamere e dispositivi di ascolto avete installato. Non importa quanti addetti al controllo dei badge o quanto personale di sicurezza armato avete impiegato. Non importa quanti miliardi di dollari avete speso.

Un cecchino o un dinamitardo che agiscono in solitaria troveranno sempre una folla come bersaglio.

Con questo non intendo dire che guardie e telecamere siano inutili, ma solo che hanno i propri limiti. Il denaro investito in questo tipo di risorse raggiunge presto il punto dei rendimenti decrescenti, e da lì in poi sono solo soldi sprecati.

Sarebbe stato molto più efficace spendere molto di quel miliardo e mezzo di dollari in intelligence e in servizi di pronto intervento in caso di emergenze. L'intelligence è uno strumento inestimabile contro il terrorismo, e funziona a prescindere da ciò che i terroristi stanno architettando -- anche se i loro piani non hanno nulla a che vedere con i giochi olimpici. La capacità e la preparazione ad intervenire prontamente in caso di un'emergenza è altrettanto importante, e anch'essa funziona a prescindere da quel che riescono a provocare i terroristi prima, durante o dopo i giochi olimpici.

Quest'anno alle Olimpiadi non sono capitati gravi incidenti di sicurezza. Come conseguenza, le più importanti aziende fornitrici di sicurezza sbandiereranno ai quattro venti questo risultato come prova che quel miliardo e mezzo di dollari è stato un ottimo investimento. Quel che in realtà si evince è con quale velocità sia facile sprecare un miliardo e mezzo di dollari in misure di sicurezza. Ora che le Olimpiadi sono finite e che tutti sono tornati a casa, il mondo non sarà più sicuro per aver speso tutti quei soldi. È un peccato, perché quel miliardo e mezzo di dollari, se investito con oculatezza, avrebbe potuto portare al mondo molta più sicurezza.

Gli articoli a riguardo:

<<http://www.cnn.com/2004/TECH/08/10/olympics.security.ap/index.html>>

<<http://www.elecdesign.com/Articles/ArticleID/8484/8484.html>>

<<http://cryptome.org/nyt-athens.htm>>

<<http://www.smh.com.au/olympics/articles/2004/07/27/1090693966896.html>>

<[http://www.news24.com/News24/Olympics2004/OutsideTrack/0,,2-1652-](http://www.news24.com/News24/Olympics2004/OutsideTrack/0,,2-1652-1655_1574262,00.html)

[1655_1574262,00.html](http://www.news24.com/News24/Olympics2004/OutsideTrack/0,,2-1652-1655_1574262,00.html)> oppure <<http://makeashorterlink.com/?V1E651849>>

Una versione di questo intervento è apparsa originariamente nel Sydney Morning Herald, durante le Olimpiadi:

<<http://smh.com.au/articles/2004/08/25/1093246605489.html>>

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

Crittanalisi di MD5 e SHA

Il mese scorso, alla CRYPTO Conference a Santa Barbara, California, dei ricercatori hanno annunciato parecchie vulnerabilità nelle funzioni hash comuni. Questi risultati, pur essendo significativi da un punto di vista matematico, non sono motivo di allarme. In ogni caso, comunque, è forse giunto il momento che la comunità di crittografi si riunisca e crei un nuovo standard hash.

Le funzioni hash one-way sono un costrutto crittografico utilizzato in svariate applicazioni. Vengono usate congiuntamente ad algoritmi di chiave pubblica, sia per la crittografia che per le firme digitali. Vengono usate nella verifica di integrità. Vengono usate nel processo di autenticazione. Presentano tutta una serie di applicazioni in una grande varietà di protocolli. Molto più degli algoritmi di crittografia, le funzioni hash one-way sono i veri "cavalli da lavoro" della crittografia moderna.

Nel 1990 Ron Rivest inventò la funzione hash MD4. Nel 1992 migliorò la funzione MD4 e sviluppò un'altra funzione hash: MD5. Nel 1993 la National Security Agency pubblicò una funzione hash molto simile alla MD5, chiamata SHA (Secure Hash Algorithm). In seguito, nel 1995, riferendosi a una vulnerabilità appena scoperta e su cui si rifiutò di divulgare informazioni, la NSA effettuò un cambiamento a SHA. Il nuovo algoritmo fu chiamato SHA-1. Oggi SHA-1 è la funzione hash più diffusa, e MD5 è ancora usata nelle applicazioni più vecchie.

Le funzioni hash one-way dovrebbero avere due proprietà. La prima è che sono a senso unico (one way): questo significa che è semplice prendere un messaggio e calcolarne il valore hash, ma è impossibile prendere un valore hash e ricreare il messaggio originale (con "impossibile" intendo dire "che non può essere fatto in un intervallo di tempo ragionevole"). La seconda proprietà è che sono libere da collisioni. Ciò significa che è impossibile trovare due messaggi che producano lo stesso identico valore hash. Il ragionamento crittografico che sta dietro a queste due proprietà è piuttosto sottile, ed invito i lettori più curiosi ad approfondire l'argomento sul mio libro "Applied Cryptography".

Rompere una funzione hash significa dimostrare che una di quelle due proprietà, o entrambe, non sono vere. La crittanalisi della famiglia di funzioni hash MD4 è andata avanti a sbalzi negli ultimi dieci anni, con risultati applicabili a versioni semplificate degli algoritmi e risultati parziali sull'algoritmo completo. Quest'anno, Eli Biham e Rafi Chen e, distintamente, Antoine Joux, hanno annunciato dei risultati crittografici davvero sorprendenti per quanto riguarda MD5 e SHA. Sono state dimostrate delle collisioni in SHA, e pare vi siano delle voci (non ancora confermate al momento) di risultati a fronte di SHA-1.

L'importanza di questi risultati dipende da chi siete. Se siete un crittografo, si tratta di una cosa enorme. Pur non essendo rivoluzionari, questi risultati rappresentano passi avanti sostanziali in questo campo. Le tecniche descritte dai ricercatori saranno probabilmente destinate ad avere altre applicazioni, e di conseguenza sarà meglio essere in grado di progettare sistemi sicuri. Questo è il modo con cui la scienza crittografica procede: si impara a ideare nuovi algoritmi rompendo altri algoritmi. In più, gli algoritmi provenienti dalla NSA vengono considerati una specie di scienza aliena: giungono da una razza superiore e senza spiegazioni alcune. Una qualsiasi crittanalisi che ha buon esito contro un algoritmo della NSA è un dato interessante nell'eterna questione di quanto siano davvero in gamba là dentro.

Per un utente di sistemi crittografici (la maggior parte dei lettori, presumo), queste novità sono importanti, ma non particolarmente preoccupanti. MD5 e SHA non si trovano ad essere improvvisamente insicuri. Nessuno violerà firme digitali né leggerà messaggi cifrati tanto presto usando queste tecniche. L'universo elettronico non è meno sicuro di quanto non lo fosse prima di questi annunci.

Ma c'è un vecchio detto all'interno della NSA: "Gli attacchi diventano ogni giorno migliori; non peggiorano mai". Queste tecniche continueranno a migliorare, e forse un giorno ci saranno attacchi pratici basati su di esse.

È venuto il momento per tutti di abbandonare SHA-1.

Fortunatamente ci sono delle alternative. Il NIST (National Institute of Standards and Technology) offre già degli standard per funzioni hash più lunghe e più difficili da rompere: SHA-224, SHA-256, SHA-384 e SHA-512. Sono già standard governativi e possono già essere usate. Questo è un ottimo tappabuchi, ma mi piacerebbe vedere dell'altro.

Mi piacerebbe vedere il NIST indire e orchestrare una competizione mondiale per la creazione di una nuova funzione hash, così come fecero per fare in modo che il nuovo algoritmo crittografico AES rimpiazzasse DES. Il NIST dovrebbe pubblicare una richiesta di algoritmi, e condurre una serie di turni d'analisi, in cui la comunità esamina le varie proposte con lo scopo di stabilire un nuovo standard.

Moltissime delle funzioni hash che abbiamo, e tutte quelle d'uso più comune, sono basate sui principi generali di MD4. Abbiamo senza dubbio imparato moltissime cose sulle funzioni hash negli ultimi dieci anni, e credo che si possa iniziare ad applicare queste conoscenze per creare qualcosa di ancor più sicuro.

Meglio farlo ora, quando non c'è alcuna ragione di farsi prendere dal panico, che non fra qualche anno, quando potrebbe esserci.

<http://news.com.com/Crypto+researchers+abuzz+over+flaws/2100-1002_3-5313655.html>
oppure <<http://makeashorterlink.com/?Z3F612849>>
<<http://www.freedom-to-tinker.com/archives/000661.html>>
<<http://www.mail-archive.com/cryptography%40metzdowd.com/msg02554.html>>
oppure <<http://makeashorterlink.com/?Q20743849>>

Informazioni tecniche:

<<http://www.cs.technion.ac.il/users/wwwb/cgi-bin/tr-get.cgi/2004/CS/CS-2004-09.ps.gz>>
oppure <<http://makeashorterlink.com/?O11735849>>
<<http://www.cs.technion.ac.il/~biham/Reports/Slides/invited-talk-sac-2004.ps.gz>> oppure
<<http://makeashorterlink.com/?T23731849>>

La parte dedicata a SHA sul sito del NIST:

<<http://csrc.nist.gov/CryptoToolkit/tkhash.html>>

Questo articolo è apparso originariamente su ComputerWorld:

<<http://www.computerworld.com/printthis/2004/0,4814,95343,00.html>>

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

Le ristampe di Crypto- Gram

Crypto- Gram è attualmente al suo settimo anno di pubblicazione. I numeri precedenti coprono tutta una serie di argomenti legati alla sicurezza e si possono trovare a questo indirizzo: <<http://www.schneier.com/crypto-gram.html>>. Quella che segue è una selezione di articoli apparsi in questo mese gli anni scorsi.

Incidenti fortuiti e incidenti di sicurezza:

<<http://www.schneier.com/crypto-gram-0309.html#1>> (originale)
<<http://www.cryptogram.it/settembre03.htm#a1>> (traduzione)

Worm benigni:

<<http://www.schneier.com/crypto-gram-0309.html#8>> (originale)
<<http://www.cryptogram.it/settembre03.htm#a8>> (traduzione)

Numero speciale sull'11 settembre, comprendente articoli sulla sicurezza negli aeroporti, sulla biometrica, sulla crittografia, la steganografia, gli insuccessi dell'intelligence, e sulla protezione della libertà:

<<http://www.schneier.com/crypto-gram-0109a.html>>

L'Esposizione Totale e la Finestra di Esposizione:

<<http://www.schneier.com/crypto-gram-0009.html#1>>

Open Source e sicurezza:

<<http://www.schneier.com/crypto-gram-9909.html#OpenSourceandSecurity>>
oppure <<http://makeashorterlink.com/?U25716849>>

Fattorizzare un numero a 512 bit:

<<http://www.schneier.com/crypto-gram-9909.html#Factoringa512-bitNumber>>
oppure <<http://makeashorterlink.com/?J17752849>>

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

Il programma Trusted Traveler

Se state partendo dall'aeroporto Logan e non avete intenzione di togliervi le scarpe al checkpoint né volete che il vostro bagaglio venga aperto, fate attenzione. Il governo degli Stati Uniti sta testando il suo programma "Trusted Traveler", e Logan è il quarto aeroporto di prova. Al momento possono aderire soltanto i frequent flier delle linee americane, ma se tutto va bene il programma sarà esteso a più persone e a più aeroporti.

I partecipanti danno il proprio nome, indirizzo, numero di telefono, data di nascita, una serie di impronte digitali e una scansione della retina. Queste informazioni vengono confrontate sui database delle forze dell'ordine e dell'intelligence. Se il candidato non è su nessuna watch list di sospetti terroristi, ed è quindi un onesto cittadino, ottiene una tessera che gli permette l'accesso a una sorta di corsia preferenziale di sicurezza. Qui saranno ancora presenti il metal detector e le macchine a raggi X per la scansione del bagaglio a mano, ma non verranno effettuati controlli ulteriori e più approfonditi a meno che non vi sia un allarme di qualche tipo.

Purtroppo questo programma non ci renderà più sicuri. Alcuni terroristi saranno in grado di ottenere tessere Trusted Traveler, e sapranno in anticipo che saranno sottoposti a controlli meno scrupolosi.

Dall'11 settembre 2001 in poi, la sicurezza degli aeroporti ha sottoposto le persone a controlli speciali: a volte prendendo individui a caso, altre volte basandosi su profili analizzati da un computer secondo determinati criteri. Ad esempio, quelle persone che acquistano biglietti di sola andata, o che pagano in contanti, verranno con ogni probabilità segnalate per essere sottoposte a ulteriori controlli.

In alcuni casi i risultati sono curiosi. La sicurezza si è trovata a perquisire bambini e persone in carrozzina. Nel 2002 Al Gore è stato casualmente fermato e controllato due volte nella stessa settimana. E proprio il mese scorso, il senatore Ted Kennedy è stato segnalato (e gli è stato negato l'imbarco) perché il computer ha deciso che il suo nome si trovava su una qualche "no-fly list".

Perché sprecare tempo prezioso facendo svuotare la borsetta a Nonna Lillie del Worchester, quando si può controllare il bagaglio a mano di Anwar, un 26enne arrivato dall'Egitto lo scorso mese e che sta viaggiando senza altri bagagli?

E il motivo è la sicurezza. Immaginate di essere un terrorista che sta pianificando un attacco e avete a vostra disposizione una mezza dozzina di uomini. Tutti fanno richiesta della tessera, e tre di loro ne ottengono una. Indovinate chi saranno i tre ad andare in missione? E questi naturalmente compreranno biglietti di andata e ritorno con carta di credito, e avranno con sé un quantitativo "normale" di bagagli.

Ciò che il programma Trusted Traveler produce è creare due diversi percorsi di accesso all'interno dell'aeroporto: massima sicurezza e minima sicurezza. L'idea è che solo le brave persone entreranno nella corsia di minima sicurezza, e che i malviventi saranno costretti ad entrare nella corsia di massima sicurezza, ma raramente cose del genere funzionano così. È necessario presumere che i malviventi troveranno un modo per entrare nella corsia a minima sicurezza.

Il programma Trusted Traveler è basato sul mito, assai pericoloso, secondo cui i terroristi corrispondano ad un certo profilo, e che si possa essere in grado di individuare i terroristi in una folla dopo aver identificato tutte le persone. Questo è semplicemente falso. Molti dei terroristi dell'11 settembre erano individui sconosciuti, e non appartenenti a nessuna watch list. Prima di far saltare il palazzo federale di Oklahoma City, Timothy McVeigh era un probato cittadino statunitense. I bombardieri suicidi palestinesi in Israele sono persone normali e non classificabili. I rapporti dell'Intelligence indicano che al Qaeda sta reclutando terroristi non arabi per le sue operazioni negli USA. La sicurezza negli aeroporti risulta più efficace disponendo guardie intelligenti che

possano notare comportamenti sospetti, e non guardie ottuse che seguano pedissequamente i risultati di un programma Trusted Traveler.

Per di più, non c'è alcun bisogno di un simile programma. I frequent flier e i viaggiatori di prima classe hanno già accesso a corsie preferenziali che permettono di evitare lunghe code ai checkpoint di sicurezza, e pare che i computer non li segnalino mai per sottoporli a controlli speciali. E ormai anche le lunghe code non sono poi molto lunghe. Sono partito dall'aeroporto Logan più e più volte, e non ho mai dovuto aspettare più di dieci minuti al checkpoint. Le persone che potrebbero fare uso della tessera non ne hanno bisogno, ed è improbabile che i viaggiatori occasionali si prenderanno il disturbo (o pagheranno la tariffa) per averne una.

Malgrado appaia un metodo tutt'altro che intuitivo, è preferibile una sicurezza che effettui controlli casuali sulle persone, e non fermare la gente solo in base a un profilo. Ed è ancora più intelligente mettere in pratica un po' di entrambi i sistemi: controlli casuali e controlli basati su profili. Ma creare una corsia di minima sicurezza, che garantisca dei controlli meno rigorosi a chi la percorre, è come invitare i malviventi ad usarla.

Questo articolo è originariamente apparso sul Boston Globe:

<http://www.boston.com/news/globe/editorial_opinion/oped/articles/2004/08/24/an_easy_path_for_terrorists/> oppure <<http://makeashorterlink.com/?E2E224939>>

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

Note di sicurezza da ogni dove: la sicurezza dei musei

Il furto dei dipinti di Munch avvenuto al Museo Munch di Oslo mette in luce una questione interessante: i requisiti di sicurezza e di pubblico accesso di famose opere d'arte contrastano fra loro e sono semplicemente incompatibili. Il livello di sicurezza che lo Smithsonian offre allo Hope Diamond non è paragonabile, e la maggior parte dei musei non possiede budget sufficiente ad offrire una simile sicurezza.

È un problema di sicurezza interessante. Gli oggetti conservati nei musei, specialmente le opere d'arte, hanno un valore inestimabile. Oggetti meno raffinati hanno meno valore, ma vengono facilmente rivenduti (basti pensare a tutti i manufatti mesopotamici rubati dai musei iracheni dopo l'invasione delle truppe USA). Ma quegli oggetti di maggior valore, in primis le opere d'arte, sono immediatamente riconoscibili e quindi perdono molto del loro valore quando vengono rubati. Occorre trovare un collezionista d'arte molto particolare che desideri un'opera che non potrà mai mostrare pubblicamente.

Gli oggetti conservati nei musei possono anche essere sottratti per chiederne un riscatto, o deturpati come atto di protesta.

Tutto questo significa che le opere d'arte nei musei devono essere protette. Ma moltissimi musei non possono permettersi il livello di sicurezza necessario a salvaguardare tali opere (persino un'assicurazione va spesso oltre i limiti di budget di un museo). E, allo stesso tempo, le opere devono poter essere visibili al pubblico, il che rende la questione sicurezza ancor più complicata.

La scelta sembra ricadere su buone serrature alle porte e su buoni allarmi, e a volte su turni di guardia che coprono le 24 ore. Questo genere di sicurezza funziona nella maggior parte dei casi, ma di tanto in tanto assistiamo a qualche spettacolare fallimento.

E, ancora peggio, la prevalenza di un buon servizio di sicurezza nelle ore notturne può avere come conseguenza l'uso, da parte dei ladri, di più violenti sistemi di intrusione per raggiungere i loro scopi.

<http://abcnews.go.com/wire/Entertainment/ap20040823_1236.html>
<<http://news.bbc.co.uk/1/hi/world/europe/3588282.stm>>

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

News

Alcuni link su come trasformare i telefoni cellulari in dispositivi di ascolto:

<http://www.netline.co.il/CAA_product.htm>
<<http://www.advanced-intelligence.com/audio.html?1586>>
<<http://seclists.org/lists/politech/2002/May/0087.html>>
<http://www.endoacustica.com/spy_telephone.htm>
<<http://www.spyshop.co.uk/basket/page08.htm>>

Telefoni che vanno in modalità "ghost":

<http://www.endoacustica.com/spy_telephone.htm>
<<http://www.gmspy.com/>>

Basta disattivare la suoneria di questo telefono, e si avrà un dispositivo di ascolto senza bisogno di altre modifiche:

<http://www.sanyo.com/wireless/handsets/downloads/PCS-4700_single.pdf>
oppure <<http://makeashorterlink.com/?Z3A712849>>

Lo scorso mese ho segnalato questo hard disk esterno crittografato, e mi domandavo perché non fossero disponibili adeguate lunghezze di chiave. O mi sono sfuggite quando ho consultato il sito, oppure le hanno aggiunte di recente: sono disponibili con crittografia DES a 40 e 64 bit, con crittografia triple DES a 128 bit, e crittografia AES a 128 e 192 bit. Sembra proprio un ottimo prodotto.

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

Un resoconto affascinante sugli usi e i limiti dell'interrogatorio:

<<http://www.cia.gov/csi/studies/vol48no1/article06.html>>

Pare che TUTTI gli utenti di Windows XP saranno in grado di scaricare e installare l'aggiornamento SP2, che possiedano di una copia legale del sistema operativo o no. Queste sono buone notizie per la sicurezza di Internet:

<<http://finance.lycos.com/home/news/story.asp?story=42933801>>

Un altro falso allarme in un aeroporto:

<<http://www.placidaudio.com/dfwshutdown.html>>

Un'analisi sul port knocking:

<<http://software.newsforge.com/software/04/08/02/1954253.shtml>>

Un buon articolo sulla cyber- assicurazione:

<http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss446_art920,00.html>
oppure <<http://makeashorterlink.com/?S1C721849>>

Un documento FBI lungo ed affascinante sull'occultazione delle armi. Comprende fotografie e immagini ai raggi X:

<<http://datacenter.ap.org/wdc/fbiweapons.pdf>>

Discussione di sicurezza sulla tecnologia dei supermercati con casse automatizzate:

<<http://www.eweek.com/article2/0,1759,1632986,00.asp>>

Un impiegato dell'Agenzia delle Entrate canadese (quella branca governativa che si occupa delle tasse) voleva contestare una multa per eccesso di velocità. Per cui ha fatto pervenire una finta nota di controllo fiscale all'agente di polizia che lo aveva multato. La causa per la contestazione della multa è stata messa in programma lo stesso giorno in cui l'agente di polizia avrebbe dovuto presentarsi per il controllo fiscale.

<http://www.thestar.com/NASApp/cs/ContentServer?pagename=thestar/Layout/Article_Type1&c=Article&cid=1092694223071&call_pageid=968332188492&col=968793972154> oppure
<<http://makeashorterlink.com/?D2D721849>>

Vulnerabilità nell'autenticazione nel sistema EAS (Emergency Alert System) di allarme emergenza degli Stati Uniti:

<<http://www.securityfocus.com/news/9324>>

La Federal Reserve è in procinto di muovere capitali via Internet. Mamma mia!

<<http://www.nypost.com/business/18671.htm>>

Il tempo trascorso prima che un PC senza patch e collegato a Internet venga attaccato con successo ammonta in media a 20 minuti. Come dimostra questo articolo, non è un intervallo di tempo sufficiente nemmeno a scaricare le patch che occorrono per la sicurezza.

<http://news.com.com/Study%3A+Unpatched+PCs+compromised+in+20+minutes/2100-7349_3-5313402.html> oppure <<http://makeashorterlink.com/?G6E722849>>
<http://www.gcn.com/vol1_no1/daily-updates/26967-1.html>

Intervista all'autore dei worm Netsky e Sasser:

<http://reviews-zdnet.com.com/AnchorDesk/4520-7297_16-5501940.html>

C'è un worm cinese che tenta di rubare esami, presumibilmente perché esiste un mercato nero a cui venderli:

<http://www.theregister.co.uk/2004/08/26/exam_virus/>

La crittografia è condannata? Malgrado il titolo sensazionalistico di questo articolo, la risposta è no. Non aspettatevi che cose del genere abbiano la benché minima importanza nel breve termine.

<http://www.technologyreview.com/articles/04/09/wo_garfinkel090104.asp>
oppure <<http://makeashorterlink.com/?A50823849>>

Una recensione articolata ed interessante di Windows XP SP2, che comprende un elenco di opportunità mancate che avrebbero aumentato la sicurezza. Una lettura consigliata:

<http://www.theregister.co.uk/2004/09/02/winxpsp2_security_review/>

Qui si possono trovare commenti molto estesi:

<<http://it.slashdot.org/it/04/09/03/1842252.shtml?tid=201&tid=128>>

Un articolo affascinante sulla contraffazione in Canada:

<http://www.canadianbusiness.com/features/article.jsp?content=20040830_61496_61496#>
oppure <<http://makeashorterlink.com/?M22832849>>

Un altro episodio della serie "un'informazione libera è più sicura di un'informazione segreta". Una commissione scientifica ha concluso che il valore derivato dal libero scambio di dati su batteri nocivi, in modo che si possano produrre vaccini e trattamenti curativi, ha un peso maggiore rispetto al pericolo rappresentato dal possibile uso di queste informazioni da parte di bioterroristi.

<<http://www.cnn.com/2004/HEALTH/09/09/bioterrorism.openness.ap/index.html>> oppure
<<http://makeashorterlink.com/?K43835849>>

Per ragioni trascurabili, questa persona si è ritrovata con due numeri di telefono identici ma con prefissi diversi: 040 1234567 e 050 1234567. Ha potuto fare questo perché il secondo operatore (che ha il secondo prefisso) gli ha dato la possibilità di scegliersi il numero.

Ciò che egli ha notato è il fatto seguente: se qualcuno ha memorizzato uno dei suoi due numeri (ma non entrambi) nella propria rubrica telefonica, e lui chiama questo qualcuno dall'altro numero, la funzione di identificazione chiamata del cellulare lo identifica correttamente in ogni caso. Questo accade anche con i messaggi di testo.

Quindi pare che i telefoni cellulari non controllino TUTTO il numero quando lo confrontano con i nominativi in rubrica.

Tutto ciò invita a un attacco spoofing molto semplice: l'aggressore attiva un numero di telefono cellulare con un prefisso diverso dalla sua vittima, ma fa in modo che il numero di telefono sia lo stesso. L'aggressore può poi chiamare e inviare messaggi ai contatti della vittima, spacciandosi per lui/lei.

Affascinante.

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

La cosiddetta "No- Fly List"

Immaginate un elenco di sospetti terroristi talmente pericolosi che non è possibile farli volare, ma allo stesso tempo così innocenti da non poter essere arrestati, nemmeno grazie ai provvedimenti draconiani del Patriot Act.

Si tratta della cosiddetta "No- Fly List" del governo federale (cioè, letteralmente, "lista di interdizione al volo"). Messa in circolazione dapprima nelle settimane successive all'11 settembre 2001 come strumento antiterrorismo, e i cui dettagli sono coperti dal segreto. Ma dato che questo elenco è pieno di errori e di ambiguità, migliaia di americani innocenti e rispettosi della legge sono stati sottoposti a lunghissimi interrogatori e a controlli invasivi ogni volta che prendono un aereo, e a volte è persino stato negato loro il permesso di imbarco. Questo elenco è stato un fallimento completo, e non ha prodotto l'arresto di nessun terrorista, da nessuna parte.

Al contrario, la lista ha messo in trappola Asif Iqbal, un uomo d'affari di Rochester, New York, che ha lo stesso nome di un sospetto terrorista tenuto attualmente in custodia a Guantanamo. Altre vittime della lista: un insegnante inglese 71enne in pensione; un uomo con un'autorizzazione governativa top-secret; una donna il cui nome è simile a quello di un australiano di 20 anni più giovane. Chiunque si chiami David Nelson è nell'elenco. La vittima più recente è il senatore Ted Kennedy, che ha avuto la sfortuna di avere un nome identico all'alias "T Kennedy" usato una volta da un tizio che qualcuno ha poi deciso dovesse essere compreso nella lista.

Per chi si trova sulla lista non c'è ricorso, e le loro storie assumono rapidamente sfumature kafkiane. Le persone possono essere inserite nell'elenco per una qualsiasi ragione, non ci sono regole di base. Non esiste la possibilità di visionare eventuali prove contro di voi, né la possibilità di avere conferma di appartenere davvero alla lista. E per la maggior parte dei malcapitati non c'è modo di togliersi dall'elenco o di "provare" una volta per tutte che loro non sono i veri ricercati. Al senatore Kennedy ci sono volute tre settimane per far togliere il proprio nome dalla lista. Quelle persone che non hanno il suo potere politico hanno passato anni per cancellare invano il proprio nome.

C'è qualcosa di palesemente non-Americano in questo "libro nero" segreto del governo, che non dà diritto ad appelli o a revisioni giudiziarie. Ancora peggio, esistono prove che tale lista viene

usata come strumento di pressione politica: attivisti per la difesa dell'ambiente, pacifisti e attivisti contro il libero scambio, guarda caso si trovano tutti in quella lista.

Ma la sicurezza è sempre un compromesso, ed alcuni potrebbero affermare giustamente che questo genere di abusi dei diritti civili sia necessario per combattere con successo il terrorismo nel nostro paese. Il problema è che la No- Fly List non ci protegge dal terrorismo.

E non c'è solo il fatto che i terroristi non sono così stupidi da viaggiare sotto nomi riconoscibili. C'è che i molti problemi causati dalla lista, che la rendono un tale affronto alle libertà civili, la rendono anche uno strumento assai poco efficace contro il terrorismo.

Una qualsiasi watch list dove sia molto facile inserire nuovi nomi e molto difficile toglierne altri, si riempirà ben presto di falsi positivi. Questi falsi positivi finiranno col gravare su qualsiasi informazione vera presente nell'elenco, e altrettanto presto la lista non farà altro che segnalare innocenti -- che è proprio quanto sta avvenendo oggi, e che spiega perché la lista non ha prodotto ancora un arresto.

Una rapida ricerca su un elenco telefonico in Internet ha prodotto 3.400 risultati per il nome "T Kennedy" negli Stati Uniti. Visto che molte coppie hanno solo un nominativo nell'elenco, molti T Kennedy sono dei consorti non riportati. Il che fa aumentare il numero dei risultati a circa 5.000. Aggiungere "T Kennedy" alla No- Fly List è una cosa irresponsabile, specialmente perché si sapeva che era solo un alias.

Ancora peggio, questo comportamento suggerisce una tattica terroristica molto semplice: nelle comunicazioni, usare nomi comuni americani per far riferimento ad altri cospiratori. Ciò renderà la lista ancora più inutile quale strumento di sicurezza, e invece molto utile come strumento di vessazione. Possono esserci 5.000 persone chiamate "T Kennedy" negli Stati Uniti, ma ce ne sono 54.000 chiamate "J. Brown".

Le watch list possono essere un buon strumento di sicurezza, ma devono essere implementate correttamente. Dovrebbe essere più difficile aggiungere nuovi nomi di quanto lo è adesso. Dovrebbe essere possibile aggiungere nomi alla lista solo per un breve periodo di tempo. Dovrebbe essere più semplice togliere nomi dall'elenco, ed aggiungere qualificatori. Ci deve essere la possibilità di ricorrere legalmente in appello per chi, innocente, desidera eliminare il proprio nome dalla lista. Se una watch list deve essere parte di un buon sistema di sicurezza, deve esistere il concetto di manutenzione dell'elenco stesso.

Tutto ciò non è niente di nuovo, e non è difficile da realizzare. La polizia affronta problemi simili tutti i giorni, e li affronta egregiamente. La polizia svolge un lavoro migliore nell'identificare i sospetti criminali che non il governo a identificare potenziali terroristi. Pensate se la polizia, nel chiedere a un testimone di identificare un sospettato, chiedesse semplicemente se "il nome suona giusto". Niente libri fotografici con i profili dei sospettati. Nessun confronto con i sospettati allineati al muro.

In un paese costruito sui principi del giusto processo, l'attuale No- Fly List è un affronto alle nostre libertà e ai nostri diritti civili. Ed è anche pessima sicurezza.

Informazioni aggiuntive:

<<http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=12740&c=206>>
<<http://www.wired.com/news/privacy/0,1848,58386,00.html>>
<<http://www.salon.com/tech/feature/2003/04/10/capps/index.html>>
<<http://www.commondreams.org/headlines02/0927-01.htm>>
<<http://www.truthout.org/cgi-bin/artman/exec/view.cgi/6/3520>>
<<http://www.belleville.com/mld/newsdemocrat/8371700.htm>>

La storia del senatore Kennedy:

<<http://www.msnbc.msn.com/id/5765143>>
<http://abcnews.go.com/wire/US/reuters20040820_78.html>

Togliersi dalla lista usando il proprio secondo nome:
<<http://www.contracostatimes.com/mlD/cctimes/news/world/9466229.htm>>

Questo articolo è apparso originariamente in Newsday:
<<http://www.newsday.com/news/opinion/ny-vpsch253941385aug25,0,3252599.story>> oppure
<<http://makeashorterlink.com/?W29816849>>

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

Commenti dei lettori

Da: Wayne Schroeder <schroede@zuri.sdsc.edu>
Oggetto: "BOB" a bordo

Sono d'accordo su quasi tutti i suoi commenti riguardanti l'incidente in questione. Il comandante ha esagerato nel decidere di tornare a terra dopo il ritrovamento di un sacchetto con la scritta "BOB" (che avrebbe forse potuto significare "Bomb on Board", ma anche molte altre cose). Ha esagerato anche se sull'aereo si trovava, come è stato riferito, un VIP. La paura è stata eccessiva, e ha prodotto soltanto altra paura.

Ma non sono d'accordo quando lei sostiene che "la paura non renderà nessuno più sicuro", e credo valga la pena di fermarci un momento a considerare la paura e altre emozioni nel contesto delle nostre decisioni razionali.

Vi sono, come lei afferma, delle situazioni in cui la paura ci renderà meno sicuri. Ci preoccupiamo a tal punto di possibilità remote che perdiamo di vista minacce molto più pressanti. Possiamo sprecare moltissime risorse in attività totalmente inefficaci.

Ma in generale, molto spesso la paura ci rende davvero più sicuri. E lo fa con una tale frequenza ed efficacia che nemmeno ce ne accorgiamo. Quando salgo sulla mia motocicletta, avverto una sottile sensazione di paura. La paura che io possa perdere il controllo del veicolo, o che qualcuno mi possa investire, o che si stacchi una ruota, e così via. E questa paura va ad aggiungere un po' più di cautela al mio modo di pensare, e il risultato è una guida più prudente. E a quanto pare è un sistema che ha sempre funzionato bene, visto che sono 30 anni che vado in moto e sono ancora vivo.

Quando camminiamo vicino al bordo di un burrone, esitiamo. Molti fra quelli che non hanno esitato sono morti, morti ancor prima di riprodursi.

Per una gran parte, le nostre emozioni esistono oggi poiché sono stimoli efficaci che interagiscono efficacemente con gli aspetti più razionali di noi stessi, in modo da produrre sagge decisioni. E per questo che la selezione naturale le ha conservate. Un pizzico di paura, o di rabbia, o di amore, può essere una buona cosa. È quando ci dimentichiamo di far funzionare anche la nostra testa che ci mettiamo nei pasticci.

Una paura eccessiva, che obnubila la nostra capacità di giudizio, può renderci meno sicuri molto di frequente. Ma un pizzico di paura solitamente ci spingerà a conservare la nostra incolumità.

Da: mskala@ansuz.sooke.bc.ca
Oggetto: GHB

Mi spiace vedere che lo scorso numero di Crypto-Gram parli del GHB solo in termini di "droga usata per compiere abusi sessuali". Non sono stato in grado di trovare nessun riferimento autorevole, recente e di buona qualità che possa corroborare quanto dico, ma una veloce consultazione di FAQ e siti Web di persone che fanno uso di questo genere di droghe dà un certo fondamento alla mia impressione soggettiva, e cioè che le persone che si servono del GHB molto più spesso lo usano su *se stessi* invece che su altri. Può darsi che trovino piacevoli gli effetti neurologici (simili a quelli dell'alcool, ma più forti), o che cerchino di usarlo per il body building (non so esattamente come funzioni, ma unitamente a una dieta speciale dovrebbe far aumentare la massa muscolare, o qualcosa del genere).

Un paio di link sul GHB:

<<http://www.erowid.org/chemicals/ghb/>>
<<http://users.lycaeum.org/~ghbfaq/>>

La storia della "droga usata per compiere abusi sessuali" è un esempio ancora migliore dell'errata percezione dei rischi rispetto al suo consiglio di portarsi appresso un apribottiglie; gli abusi sessuali possono rappresentare statisticamente un utilizzo impopolare del GHB, ma è l'unica minaccia presa di mira da quasi tutti gli sforzi in opposizione al GHB. La legge che ha reso il GHB una sostanza controllata nella categoria Schedule I è stata chiamata "The Hillory J. Farias and Samantha Reid Date-Rape Drug Prohibition Act" (lett. "Il Prohibition Act della droga- da-stupro di Hillory J. Farias e Samantha Reid"). Il risultato è che molte persone adesso pensano che l'abuso sessuale sia la sola cosa che facciano quelli che usano il GHB. Pare che vi siano molti più casi di persone che hanno subito violenze dopo che esse stesse hanno aggiunto il GHB ai loro drink, dato che non interagisce molto bene con l'alcool, eppure non ho mai visto una campagna informativa contro questo genere di minaccia.

Da: Trammell Hudson <hudson@swcp.com>
Oggetto: GHB

Per una misura di sicurezza molto più elaborata, osservi questa invenzione di un tizio del North Wales:

<http://icnorthwales.icnetwork.co.uk/news/regionalnews/tm_objectid=14386720&method=full&siteid=50142&headline=gadget-will-stop-spiked-drink-peril-name_page.html>
oppure <<http://makeashorterlink.com/?Q1A826849>>

Da: Greg Walker <Greg.Walker@cityofhouston.net>
Oggetto: I ranger dell'aeroporto di Houston

Il programma dei Ranger Aeroportuali è un programma aggiunto di sicurezza che, dalla lettura di altri articoli del signor Schneier disponibili sul Web, sembrerebbe prodotto da quel modo di ragionare non convenzionale che normalmente Schneier difenderebbe. Devo quindi presumere che l'unico motivo per cui egli non sostiene il nostro programma sia il suo non essere pienamente consapevole della storia dell'aeroporto, né del ruolo dei Ranger Aeroportuali nel disegno generale della sicurezza.

Il signor Schneier sembra basare le sue opinioni sulla sola consultazione del programma presente nelle pagine Web dello Houston Airport System (HAS), programma che, fra l'altro, vanta più di 450 volontari che hanno superato con successo i background check. Occorre notare come non tutti i candidati siano stati considerati idonei. Credo sia piuttosto imprudente da parte mia discutere i criteri e la profondità dei nostri background check in un forum pubblico. Tuttavia, posso affermare che noi professionisti della sicurezza della HAS Public Safety & Technology Division riteniamo che esso sia ad un livello adeguato, tenendo conto che i Ranger si trovano a cavalcare sul suolo pubblico, tanto per cominciare. Sembrerebbe che il signor

Schneier sia convinto della nostra dipendenza dal programma "Ranger Aeroportuali" come mezzo primario per la sicurezza del perimetro; se così fosse, sarebbe una grave assunzione erronea. Abbiamo svariate risorse tecnologiche e professionali tra le nostre forze di sicurezza coinvolte nella protezione del perimetro, che esaminano costantemente le tecniche e le strategie più aggiornate. La legge federale mi impedisce di rivelare con maggior dettaglio le nostre tecniche attuali e su quali nuove tecniche ci stiamo appoggiando.

Il George Bush Intercontinental Airport (IAH) possiede più di 11.000 acri di terra ed è stato costruito su quella che, non molto tempo fa, era un'area rurale vicina alla Città di Houston. Si tratta di un tipo di collocazione molto comune per un aeroporto. Una vasta porzione di terra allo IAH è boschiva, e comprende un'enorme quantità di sottobosco. Si tratta di terra che viene conservata per eventuali future espansioni, ed esiste una zona di radura fra queste aree e il confine di sicurezza eretto intorno all'area delle operazioni aeroportuali. Questo territorio si trova al di fuori dell'area regolata dalle autorità federali, ed è essenzialmente suolo pubblico. Per molti anni, visto che l'area disponibile per cavalcare è stata grandemente ridotta a causa dello sviluppo che normalmente avviene intorno agli aeroporti, la comunità equestre della North Harris County ha cavalcato attorno a quest'area senza avere regolari permessi o autorizzazioni.

Lo Houston Airport System (HAS) ha ritenuto opportuno lavorare insieme alla comunità equestre invece di osteggiarla. Dopotutto la terra appartiene ai contribuenti, e il risultato è stata una situazione che ha portato benefici ad entrambe le parti. Chi va a cavallo ora ha un ottimo luogo per cavalcare, dato che lo Houston Airport System ha effettuato una serie di migliorie alla terra per incentivarne l'uso quotidiano da parte dei Ranger Aeroportuali. In cambio ora l'aeroporto sa chi sta cavalcando là fuori, conosce il loro background, e ha fatto in modo che i Ranger portino dei badge identificativi. I Ranger, grazie a telefoni cellulari, riferiscono al nostro Security Dispatch Center in merito a ogni persona da loro fermata sprovvista di badge o in merito a qualsiasi attività rilevata e ritenuta sospetta. In breve, i Ranger offrono nuovi occhi e orecchie alle forze di polizia e agli esperti di sicurezza. Non solo ricercano individui sospetti o segni di attività e ingressi non autorizzati, ma riferiscono anche di eventuale boscaglia che sta crescendo troppo vicina ai confini di sicurezza dell'aeroporto, di animali che tentano di scavare nei pressi del confine e che potrebbero introdursi nelle piste, ecc., in modo che si possano prendere delle contromisure correttive per proteggere le piste e le corsie dei taxi anche dai pericoli più comuni. I Ranger hanno riportato diversi casi di violazione territoriale e hanno impedito almeno due furti di proprietà.

Il signor Schneier è preoccupato delle libertà civili e delle difese costituzionali, unitamente al profiling su base razziale. Queste sono preoccupazioni necessarie e ammirevoli. Tuttavia i Ranger Aeroportuali non hanno il potere di arrestare o trattenere chicchessia: sono semplicemente occhi e orecchie al servizio delle forze dell'ordine e degli esperti di sicurezza. Il loro unico obbligo è osservare, prestare attenzione a determinate cose, ed eventualmente riferire via cellulare al Security Dispatch Center dell'aeroporto.

Il signor Schneier sostiene che il perimetro che circonda l'aeroporto era solito essere una terra di nessuno, e che perciò chiunque fosse passato sulla proprietà sarebbe stato immediatamente sospetto. Ah, se vivessimo in quel mondo perfetto. Nelle vicinanze dei più grandi aeroporti, oggi, sono presenti strade pubbliche, strade statali e persino autostrade, che si trovano davvero a pochi metri dal confine di sicurezza. Se l'aeroporto è fortunato e presenta parecchi acri di terra libera intorno, come è il caso del George Bush Intercontinental, allora il problema di pattugliare tutte quelle aree diventa un problema di forza lavoro. Oggi più che mai, le forze dell'ordine e le agenzie di sicurezza hanno bisogno dell'aiuto di tutti i cittadini, e il programma dei Ranger Aeroportuali (almeno all'interno del George Bush Intercontinental Airport) rende possibile tutto questo in modo molto evidente.

Come saprà meglio dirle qualsiasi corpo di polizia o agenzia di sicurezza, il crimine, e nella realtà odierna il terrorismo, viene sostanzialmente ridotto nei casi in cui vi sia una presenza visibile di forze dell'ordine, di forze di sicurezza e, sì signor Schneier, anche di cittadini, specialmente cittadini attenti e preparati, che sanno chi chiamare e che cosa riferire. Sono lieto di affermare che

le forze dell'ordine, ad ogni livello, fra cui la polizia federale e locale, appoggiano fortemente il programma, e di volta in volta offrono un addestramento aggiuntivo per i Ranger Aeroportuali.

Da: Folkert van Heusden <folkert@vanheusden.com>
Oggetto: Vulnerabilità del microcodice del processore

Lei scrive: "Pare che sia possibile aggiornare il microcodice del processore AMD K8 (Athlon64 o Opteron). E, udite udite, non c'è alcun controllo di autenticazione."

Questo è anche possibile con processori Intel Pentium Pro, II, ecc. Si veda: <<http://www.urbanmyth.org/microcode/>> per fare tutto questo sotto Linux.

Da: "Allan Dyer" <adyer@yuikee.com.hk>
Oggetto: Nota sulla privacy della CIA

Il suo commento alla nota sulla privacy redatta dalla CIA è stato "Hmmm, ma non è il loro mestiere quello di raccogliere informazioni personali senza chiedere il permesso agli interessati?"

Certo, verissimo. Ma non è forse vero che anche mentire fa parte del loro mestiere?

Da: "Hamlin, Stuart" <SHamlin@GAM.COM>
Oggetto: Windows XP SP2

Per quanto concerne le sue affermazioni in merito a Windows XP SP2, credo che lei abbia per metà ragione e per metà torto. È vero che se la riparazione di bug di sicurezza nel sistema operativo va a compromettere un'applicazione, è l'applicazione ad essere nel torto. Tuttavia, ritengo che l'altissimo numero di vittime causate dal Security Pack 2 stia raggiungendo livelli assurdi.

Si veda: <<http://support.microsoft.com/default.aspx?kbid=884130>>

Microsoft non ha mai fatto mistero che certe applicazioni potrebbero non funzionare più come prima, ma il problema è che la gente andrà a leggere quell'elenco e dirà "beh, sono tutte le applicazioni che uso" e non farà nulla. Nessuna patch di sicurezza vale tutto questo disagio causato alla maggior parte degli utenti, soprattutto alle piccole e medie imprese. Soprattutto se, fino ad oggi, sono riusciti ad evitare infezioni ed attacchi.

Naturalmente ciò che occorrerebbe non è tanto un elenco delle applicazioni colpite sul sito, ma una serie di risorse a cui far riferimento per far funzionare di nuovo quelle applicazioni. Finché Microsoft non farà una cosa del genere, suppongo che moltissime persone non installeranno SP2, e questo renderà tutti noi meno sicuri.

Ancora una volta, Microsoft fallisce in ciò che conta di più.

Da: Jim Reid <jim@rfc1035.com>
Oggetto: La preparazione all'emergenza degli inglesi

Lei ha scritto: "È un sito scherzoso, e val la pena farci un giro: <<http://www.preparingforemergencies.co.uk/>>"

Si tratta della parodia di un opuscolo che il governo del Regno Unito ha inviato ad ogni cittadino del paese. Esso contiene saggi consigli quali "In caso d'incendio, uscite di casa, state fuori e chiamate il 999" e "Nel caso esplodesse un ordigno nel vostro stabile, cercate la via d'uscita più

sicura". Grazie al cielo che il governo di Sua Maestà me lo ha detto, non avrei mai pensato di fare tutte quelle cose prima di aver letto questo opuscolo!

Il vero articolo è all'indirizzo <<http://www.preparingforemergencies.gov.uk>>. A mio modesto avviso è una tragicommedia ancora migliore della parodia. Afferma ciò che è mostruosamente ovvio: in caso di emergenza, chiamate i servizi di emergenza e ascoltate la radio e la TV per ricevere consigli e informazioni utili. Però non dice nulla su cosa fare se i telefoni, la radio e la TV non funzionano. In ogni caso, almeno qualcuno alla protezione civile ha un certo sense of humour. La postilla in fondo dice che l'opuscolo può essere copiato anche senza autorizzazione, a meno che non venga usato con intento derogatorio.

Da: BJBrooks <bobstuff17@hotmail.com>
Oggetto: FobCam

"Ecco un tizio che ha installato una webcam che inquadra il suo token SecurID, in modo che lui non debba preoccuparsi di portarselo in giro. E sapete qual è il bello? Che a meno di non sapere a chi appartiene la pagina web, si tratta di un'ottima misura di sicurezza."

È quanto da lei scritto di recente nella sua newsletter in merito all'idiota che ha il suo FOB in bella vista. Sono d'accordo con lei quando afferma che, a meno di non sapere a chi appartiene, si tratta di buona sicurezza.

In un mondo ideale, nessuno avrebbe bisogno di un FOB, ma tutto quel che ha fatto questo tizio non è altro che rendere se stesso (e, cosa più grave, la sua compagnia) un bersaglio per apprendisti hacker o ragazzi annoiati in cerca di qualcosa di divertente. Dopo aver visto quella pagina Web, nel giro di pochi minuti, avevo il nome del tizio, il suo indirizzo, 4 numeri di telefono, il nome della moglie, il nome e la data di compleanno del figlio, il nome dell'azienda, le sue qualifiche, e svariati indirizzi email. Avevo persino una foto di lui con suo figlio. E questo solo cercando in superficie. Non mi interessa aggirare il firewall della sua azienda. Ero solo curioso di vedere quando sarebbe stato difficile reperire queste informazioni. Tutti i suoi indirizzi email hanno identico nome utente. Scommetto il mio prossimo stipendio che è lo stesso nome utente che usa al lavoro. Avendo il nome di sua moglie e di suo figlio, per non parlare della data del compleanno, con il livello di originalità che ha questo tizio, sono certo che il figlio del mio vicino di casa, che ha 8 anni, sarebbe in grado di scoprire la password nel giro di un'ora.

Da: Greg Guerin <glguerin@amug.org>
Oggetto: Il commento di ICS Atlanta sui Code-Talker Navajo

La "lunghezza della chiave" dei code-talker Navajo sarebbe stata ben più grande di zero. Tutti i code-talker venivano specificatamente addestrati, e memorizzavano il significato in codice di parecchie parole-codice, le quali venivano pronunciate nella lingua nativa Dineh (Navajo). Un esempio di dizionario che ho trovato sembra combaciare con altri risultati apparsi inserendo "navajo code talker dictionary" nel motore di ricerca:

<<http://www.americanindians.com/CodeTalkersDictionary.htm>>

Già il solo sistema di sostituzione delle lettere è geniale. Un buon numero di parole in codice sono giochi di parole bilingui, come "ant fight" per "about" o "weasel tied together" per "which" (A-bout and W-hitch, capito?).

("bout" e "hitch" sono sinonimi di "fight" e "tied together", ndt)

E questo solo per quanto concerne il codice stesso. Non parliamo poi del contesto culturale condiviso da tutti i code-talker, o del fatto che tutti i messaggi in codice erano comunicati da persona a persona oralmente da parlanti di madrelingua.

