

CRYPTO-GRAM
15 giugno 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:

La scoperta dei codici iraniani
Identificazioni biometriche per il personale degli aeroporti
Le ristampe di Crypto-Gram
Microsoft e il Security Pack 2
News
Il jamming dei telefoni cellulari e gli attacchi terroristici
Fare fotografie nelle stazioni della metropolitana e gli attacchi terroristici
Le News di Counterpane
Il worm Witty
Commenti dei lettori

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

La scoperta dei codici iraniani

Ahmed Chalabi è accusato di avere informato gli iraniani del fatto che gli Stati Uniti hanno scoperto i loro codici di intelligence. Ma che cosa hanno scoperto, esattamente, gli Stati Uniti? Come hanno potuto gli iraniani verificare le dichiarazioni di Chalabi, e che cosa potrebbero fare di conseguenza?

Quanto segue è un tentativo di risposta ad alcune di queste domande.

Ogni nazione ha i suoi segreti. Negli Stati Uniti, la National Security Agency ha il compito di proteggere i segreti americani e contemporaneamente di venire a conoscenza dei segreti di altri paesi (in realtà, è la CIA ad avere l'incarico di scoprire i segreti di altri paesi in generale, mentre la NSA è incaricata di intercettare le comunicazioni elettroniche delle altre nazioni).

Per proteggere i propri segreti, l'intelligence dell'Iran -- come i leader di tutti i paesi -- comunica in codice. Non si tratta ovviamente di codici scritti a matita su carta, ma macchine con software per la crittografia. Probabilmente gli iraniani non ne hanno costruite di proprie, ma le hanno acquistate da un'azienda come l'elvetica Crypto AG. Alcune di queste macchine proteggono le conversazioni telefoniche, altre proteggono messaggi inviati via fax e telex, e altre ancora proteggono le comunicazioni via computer.

In quanto comuni cittadini privi di autorizzazioni speciali, non sappiamo quali codici di quali macchine la NSA abbia compromesso, né sappiamo come abbia fatto. È possibile che gli Stati Uniti abbiano decodificato gli algoritmi di crittazione matematica utilizzati dagli iraniani, come fecero gli inglesi e i polacchi con i codici tedeschi durante la Seconda Guerra Mondiale. È anche possibile che la NSA abbia installato una backdoor nelle macchine iraniane. Si tratta in sintesi di una falla deliberatamente collocata a livello di crittografia che permette, a chiunque ne sia a conoscenza, di leggere i messaggi.

Vi sono altre possibilità: la NSA potrebbe avere avuto un infiltrato all'interno dell'intelligence iraniana che ha passato le impostazioni di crittografia necessarie a leggere i messaggi. John Walker aveva venduto per anni ai sovietici questo genere di informazioni sui codici navali statunitensi, durante gli scorsi Anni Ottanta. Oppure gli iraniani potrebbero aver avuto delle procedure crittografiche un po' troppo approssimative, che hanno permesso alla NSA di decodificare la crittazione.

Ovviamente, la NSA deve intercettare i messaggi in codice per poterli decifrare, ma per questo hanno tutta una serie di punti di ascolto sparsi in tutto il mondo. La maggioranza delle comunicazioni avviene attraverso onde radio, microonde, ecc. -- e può essere facilmente intercettata. Quelle comunicazioni che avvengono invece via cavo interrato sono molto più difficili da intercettare, e occorre che vi sia fisicamente qualcuno in Iran per effettuare l'intercettazione. Ma la ragione per cui vengono utilizzate macchine per la crittazione è proprio quella di poter inviare messaggi attraverso canali non sicuri e impercettibili, perciò è molto probabile che la NSA avesse da leggere un flusso costante di messaggi dell'intelligence iraniana.

A prescindere dalle metodologie, si tratterebbe di un enorme "colpo" di intelligence da parte della NSA. Era anche un segreto esso stesso. Se gli iraniani avessero saputo che la NSA stava leggendo i loro messaggi, avrebbero cessato di usare le macchine per la crittazione, ormai penetrate, e la fonte da cui la NSA attingeva i segreti iraniani si sarebbe prosciugata. Il segreto per cui la NSA poteva leggere i segreti iraniani era molto più importante di un qualsiasi segreto iraniano scoperto o scopribile dalla NSA.

La conseguenza: spesso gli Stati Uniti vengono a conoscenza di segreti sui quali non possono agire, poiché una qualsiasi azione svelerebbe il loro segreto. Durante la Seconda Guerra Mondiale, gli Alleati avrebbero fatto di tutto per evitare che i tedeschi si rendessero conto che i loro codici erano ormai scoperti. Gli Alleati conoscevano la posizione degli U-Boot, ma non avrebbero bombardato gli U-Boot prima di scoprirli con altri mezzi più evidenti... altrimenti i nazisti avrebbero potuto insospettirsi.

C'è una storia riguardante Winston Churchill e i bombardamenti di Coventry: presumibilmente egli era a conoscenza che la città sarebbe stata bombardata, ma non poté avvertirne i cittadini. La storia è apocrifia, ma è un buon esempio delle misure estreme a cui le nazioni ricorrono per proteggere il loro segreto, cioè che sono in grado di sapere i segreti dei nemici.

E vi sono molte storie di errori e passi falsi. Nel 1986, dopo il bombardamento di una discoteca di Berlino, l'allora presidente Reagan dichiarò di essere in possesso di prove inconfutabili che dietro all'attacco ci fosse il leader Gheddafi. L'intelligence libica si rese conto che i propri codici diplomatici erano stati scoperti, e li modificò. Il risultato fu una grande battuta d'arresto per l'intelligence statunitense, tutto per qualche parola di troppo.

Presumibilmente, l'intelligence iraniana ha provato a verificare le dichiarazioni di Chalabi inviando un messaggio riguardante un certo nascondiglio per armamenti. Se gli Stati Uniti avessero agito sfruttando questa informazione, gli iraniani avrebbero capito che i propri codici erano stati scoperti. Ma gli Stati Uniti non hanno fatto nulla, il che dimostra che su questo aspetto sono stati molto accorti. Forse sapevano che gli iraniani si erano insospettiti, o forse erano in attesa di inventarsi una ragione fittizia, ma plausibile, che spiegasse come mai fossero al corrente del nascondiglio di munizioni.

Così adesso il segreto della NSA è scoperto. Gli iraniani hanno senza dubbio cambiato le loro macchine per la crittazione, e la NSA ha perduto la fonte dei segreti iraniani. Ma non si sa molto altro. Chi ha informato Chalabi? Solo pochissime persone potevano conoscere questo importante segreto americano, e la spia è certamente colpevole di tradimento contro lo stato. Forse Chalabi non ha mai saputo nulla, e non ha mai informato gli iraniani. Forse gli iraniani lo hanno capito in qualche altro modo, e fingono che sia stato Chalabi ad informarli, così possono proteggere qualche altra loro fonte di intelligence.

Durante gli scorsi Anni Cinquanta, gli americani fecero degli scavi nel sottosuolo di Berlino Est per effettuare intercettazioni via cavo. Hanno ricevuto ogni genere di informazione di intelligence, finché i tedeschi dell'est non hanno scoperto il tunnel. Tuttavia, i sovietici erano al corrente dell'operazione fin dall'inizio, poiché una loro spia era presente nelle fila dell'intelligence Britannica. Ma non poterono fermare gli scavi, perché altrimenti avrebbero rivelato la presenza di George Blake come loro spia.

Se gli iraniani sapevano che gli Stati Uniti sapevano, perché non hanno fatto finta di non sapere, fornendo così false informazioni agli Stati Uniti? O forse lo hanno sempre fatto, da anni, e gli USA hanno finalmente capito che gli iraniani già sapevano. Forse gli Stati Uniti sapevano che gli iraniani sapevano, e stanno sfruttando tutto questo per gettare discredito su Chalabi.

La cosa davvero peculiare di questa storia è che gli USA sono già stati accusati di aver agito in tal modo contro l'Iran. Nel 1992, l'Iran arrestò Hans Buehler, un dipendente della Crypto AG, poiché si sospettava che la Crypto AG avesse installato delle backdoor sulle macchine per la crittazione vendute all'Iran -- su richiesta della NSA. Buehler dichiarò la sua innocenza dopo ripetuti interrogatori, e venne finalmente rilasciato nove mesi dopo, nel 1993, quando la Crypto AG pagò un milione di dollari per la sua libertà -- per poi prontamente licenziarlo e fatturargli la somma spesa per il rilascio. A questo punto, Buehler iniziò a fare domande imbarazzanti sui rapporti fra la Crypto AG e la NSA.

Per cui può darsi che le informazioni di Chalabi risalgano al 1992 e che gli iraniani abbiano cambiato le loro macchine per la crittazione una decina d'anni fa.

O forse la NSA non ha mai decodificato il codice dell'intelligence iraniana, e tutta questa storia non è altro che un grosso bluff.

In questo vago mondo di giochi al gatto col topo e di persecuzioni, è difficile essere sicuri di qualsiasi cosa.

La storia di Hans Buehler:

< <http://www.aci.net/kalliste/speccoll.htm> >

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

Identificazioni biometriche per il personale degli aeroporti

Ho scritto molto in merito a documenti d'identità e dati biometrici: su come non funzionino e su come non migliorino la sicurezza. È bello poter scrivere finalmente qualcosa su un tipo di identificazione biometrica davvero efficace.

Alcuni membri del Congresso stanno facendo pressioni sulla TSA -- cioè quelli che gestiscono la sicurezza negli aeroporti -- per sviluppare documenti identificativi biometrici per quel milione di individui che compongono il personale di aeroporti, porti, e scali merci ferroviari.

Questa è la maniera corretta di usare un documento identificativo biometrico. Il punto forte della biometria è l'autenticazione: questa persona è davvero chi dice di essere? Realizzare documenti identificativi a persone che necessitano di accedere a queste aree vitali è una mossa intelligente, e servirsi della biometria per rendere questi documenti più difficili da contraffare è ancora più acuto. Non si parla di estesa sorveglianza della popolazione; non sono in ballo questioni sui diritti civili o di privacy.

Gli impiegati dei trasporti sono un anello debole nella sicurezza degli aerei. Si stanno spendendo miliardi su programmi per la creazione di profili dei passeggeri come il CAPPS-II, ma nessuna di queste contromisure potrà essere efficace se i terroristi possono semplicemente aggirare i sistemi. L'attuale politica della TSA è che i dipendenti degli aeroporti possono accedere ad aree di sicurezza degli aeroporti senza alcun controllo eccettuato un rudimentale background check. Ciò include le migliaia di individui che lavorano per i negozi e i ristoranti dei terminal degli aeroporti, nonché l'esercito di lavoratori addetti alla pulizia e alla manutenzione dei velivoli, al carico bagagli, al servizio alimentare. Chiudere questo enorme buco di sicurezza è un'ottima idea.

Tutto questo deve tuttavia essere controbilanciato dai costi. Emanare un milione di documenti identificativi, e probabilmente decine di migliaia di lettori elettronici, non sarà un'operazione a buon mercato. Ma certamente ci fornirà una sicurezza maggiore, dollaro per dollaro, rispetto ad un ennesimo sistema di sicurezza che controlla i passeggeri.

Purtroppo, gli uomini politici tendono a preferire sistemi di sicurezza che vadano a influire su vaste fette della popolazione. A loro piace quel tipo di sicurezza che sia visibile; è la prova che a loro sta davvero a cuore la sicurezza, ed è più probabile che fruttino loro qualche voto in più. Un sistema di sicurezza che coinvolge i lavoratori dei trasporti, molto più "nascosto" agli occhi del grande pubblico, probabilmente è destinato a procurare un minor supporto rispetto ad un sistema più "pubblico".

Speriamo che i legislatori americani facciano comunque la cosa giusta.

< <http://www.cnn.com/2004/TRAVEL/06/09/airport.security.ap/> >

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

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.

I rischi del cyber- terrorismo:

< <http://www.schneier.com/crypto-gram-0306.html#1> >

< <http://www.communicationvalley.it/giugno03.htm#a1> > (traduzione in italiano)

Rimediare agli insuccessi dell'intelligence:

< <http://www.schneier.com/crypto-gram-0206.html#1> >

< <http://www.communicationvalley.it/giugno02.htm#a1> > (traduzione in italiano)

Gli honeypot e il Progetto Honeynet:

< <http://www.schneier.com/crypto-gram-0106.html#1> >

Microsoft e il protocollo SOAP:

< <http://www.schneier.com/crypto-gram-0006.html#SOAP> >

performance o di funzionalità non girino sul software piratato. Microsoft intende negare certi vantaggi a chi non ha comprato i suoi prodotti, invogliando queste persone a diventare utenti con regolare licenza. Ma gli aggiornamenti di sicurezza sono una cosa diversa. Microsoft sta danneggiando i suoi utenti in regola se nega una maggior sicurezza agli utenti non in regola.

Questa decisione, più di tutto ciò che Microsoft ha detto o fatto negli ultimi anni, è per me la prova che la sicurezza non è la prima priorità dell'azienda. Questa era l'occasione per fare la cosa giusta: mettere la sicurezza davanti ai profitti. Questa era l'occasione per fare un'ottima figura con la stampa e migliorare la sicurezza di chiunque utilizzi prodotti Microsoft in tutto il mondo. Microsoft dichiara che migliorare la sicurezza è la cosa più importante, ma le sue azioni provano il contrario.

SP2 è un importante aggiornamento di sicurezza per Windows XP, e mi auguro che sia installato il più diffusamente fra gli utenti con regolare licenza di XP. Spero inoltre che venga piratato in fretta, in modo che anche chi non possiede una regolare licenza di XP possa installarlo. Se voglio rimanere sicuro in internet, mi è necessario che tutti diventino più sicuri. E più gente installerà SP2, più sarà a vantaggio di tutti.

Il report originale:

< <http://computertimes.asia1.com.sg/news/story/0,5104,2292,00.html> >

La posizione "riveduta e corretta" di Microsoft:

< http://zdnet.com.com/2100-1105_2-5209896.html >

< http://www.theregister.co.uk/2004/05/11/xpsp2_pirate_blocking/ >

Dettagli sul Service Pack 2:

< <http://www.mcpmag.com/columns/article.asp?EditorialsID=716> >

Un'idea simile:

< <http://www.securityfocus.com/printable/columnists/243> >

Questo articolo è apparso originariamente su Network World:

< <http://www.nwfusion.com/columnists/2004/0531schneier.html> >

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

News

Ottima storia di ingegneria sociale usata per un vero e proprio furto:

< <http://lineman.net/node/view/270> >

L'esperienza di una persona che ha cercato di rendere sicuro Windows. Uno spunto interessante: dopo aver fatto un'installazione pulita, non ha avuto il tempo di scaricare tutte le patch di sicurezza: il computer era già infettato da software maligno. Una lettura consigliata.

< <http://www.techuser.net/index.php?id=47> >

Una buona analisi dei rischi connessi all'hacking delle macchine per il voto elettronico:

< <http://www.cs.duke.edu/~justin/voting/PrezNader.html> >

Avi Rubin ha proposto una sfida molto interessante per la sicurezza delle macchine per il voto elettronico.

< <http://avirubin.com/vote/ita.challenge.pdf> >

Barbara Simons offre un'eccellente confutazione alla posizione della League of Women Voters sulle macchine per il voto elettronico:

< <http://www.leagueissues.org/lwvqa.html> >

Ecco la storia di un tentativo fallito di imbastire uno scandalo sessuale per coinvolgere John Kerry, e dal punto di vista della sicurezza si può notare come sia l'esempio concreto di un hacker politicamente motivato, forse la stampa: "Un'altra cosa preoccupante è stata trovare il mio account Hotmail violato, e quindi era per me impossibile consultare la mia email. Una serie casuale di persone presenti nella mia rubrica, e a cui non avevo parlato per mesi, improvvisamente hanno iniziato a ricevere chiamate da vari reporter. Mio padre mi ha chiamato per dirmi che qualcuno aveva provato a fare la stessa cosa con il suo account, ma che il suo software di sicurezza aveva intercettato queste persone, e il tracciato di rete aveva rivelato l'indirizzo di un singolo computer sito a Washington D.C."

< <http://www.newyorkmetro.com/nymag/features/coverstory/9221/index.html> >

oppure < <http://tinyurl.com/3298t> >

Sulla lista delle pessime idee: musica protetta in modo che occorran le impronte digitali corrette per poterla suonare.

< http://www.theregister.co.uk/2004/06/04/biometric_drm/ >

Gli ufficiali di aviazione sono facilmente identificabili sugli aerei:

< <http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2004/06/01/MNGLL6UR2I1.DTL> >

Come il problema dell'identità rende la sicurezza informatica così primitiva:

< <http://comment.silicon.com/0,39024711,39120567,00.htm> >

Un articolo sulle password e sulla loro sicurezza, che comprende questo interessante passaggio: "Per una maggior sicurezza, lei poi estrae una scheda che contiene 50 codici usa e getta. Jubran usa i codici, uno dopo l'altro, ogni volta che effettua un login o una transazione. La sua banca, la Nordea PLC, le invia automaticamente una nuova scheda poco prima che la precedente sia esaurita".

< <http://www.wired.com/news/infostructure/0,1377,63670,00.html> >

Come scoprire dove si trovano i laboratori illegali per la creazione di armi chimiche analizzando i loro scritti accademici pubblicati:

< <http://www.nature.com/nsu/040531/040531-1.html> >

Il personaggio fittizio di un videogioco per poco non diventa causa di un allarme terroristico nazionale:

< http://www.usnews.com/usnews/issue/040517/whispers/17whisplead_2.htm >

< <http://games.slashdot.org/games/04/05/10/2036258.shtml?tid=127&tid=133&tid=186> >

oppure < <http://tinyurl.com/2sce3> >

Gli spammer utilizzano finti messaggi con firma digitale PGP per aggirare i filtri anti-spam:

< <http://smh.com.au/articles/2004/06/01/1086058836957.html> >

< <http://www.math.org.il/PGP-JoeJob.txt> >

Articolo interessante sui rischi di dirottamento dei browser Web, nello specifico i rischi di essere incastrati per reati non commessi:

< http://www.theregister.co.uk/2004/05/13/browser_hijacking_risks/ >

< <http://www.wired.com/news/infostructure/0,1377,63391,00.html> >

Un articolo affascinante sulla sicurezza in ambito nucleare. Robert McNamara, il Segretario della Difesa degli Stati Uniti, ha aggiunto un livello di sicurezza alla procedura di lancio del missile Minuteman, proteggendola con un codice "Permissive Action Link" a 8 cifre. Ma il Comando Aereo Strategico, temendo che la ricerca e l'inserimento di questi codici possa impedire una rapida procedura di lancio dei missili, ha quietamente decretato che il codice debba sempre essere 00000000.

< <http://www.cdi.org/blair/permissive-action-links.cfm> >

rumore. Witty ha infettato solo circa 12.000 macchine, quasi nessuna di esse di proprietà di utenti domestici. Non è sembrata una gran cosa, questo Witty.

Eppure Witty è stata una gran cosa. Ha rappresentato uno dei primi software maligni davvero preoccupanti e sarà probabilmente il precursore di nuovi worm. I professionisti in ambito IT devono comprendere che cosa sia Witty e ciò che fatto.

Witty è stato il primo worm a prendere di mira uno specifico set di prodotti di sicurezza -- in questo caso BlackICE e RealSecure di ISS. Ha infettato e distrutto solamente quei computer che avevano caricate e in funzione delle specifiche versioni di questo software.

Witty ha svolto egregiamente il suo compito. Il numero di macchine esposte e vulnerabili ammontava a dodicimila unità, e Witty le ha infettate tutte -- in ogni parte del mondo -- in 45 minuti. È il primo worm a danneggiare velocemente un numero ristretto di unità. I precedenti worm che avevano come bersaglio un tale quantitativo di macchine erano tremendamente lenti (ad esempio Scalper e Slapper).

Witty è stato scritto molto rapidamente. La compagnia di sicurezza eEye ha scoperto la vulnerabilità nei prodotti di ISS, BlackICE e RealSecure, l'8 marzo, e ISS ha rilasciato una versione con patch il 9 marzo. eEye ha pubblicato una descrizione molto accurata e tecnica della vulnerabilità il 18 marzo. La sera del 19 marzo, circa 36 ore dopo la divulgazione pubblica da parte di eEye, il worm Witty veniva lasciato libero di agire.

Witty è stato scritto molto bene. La lunghezza totale non supera i 700 byte. Ha utilizzato un generatore di numeri casuali per diffondersi, evitando molti dei problemi che affliggevano i precedenti worm. Si è diffuso inviando se stesso verso indirizzi IP casuali con porte di destinazione casuali, un trucco che ha facilitato l'aggiramento dei firewall. Inoltre -- e questa è la cosa più clamorosa -- è privo di bug. Questo implica fortemente che il worm è stato testato prima del rilascio.

Witty è stato rilasciato in maniera molto astuta, attraverso un bot network di circa 100 macchine infette. Di questa tecnica si era parlato tempo fa, ma Witty è il primo caso di worm che lo ha fatto davvero sul campo. Questo, insieme alla modalità geniale con cui si è diffuso, ha fatto sì che Witty infettasse ogni host disponibile in 45 minuti.

Witty è stato eccezionalmente maligno. È stato il primo worm a larga diffusione che ha distrutto gli host che ha infettato. E lo ha fatto direi con eleganza. Il suo payload maligno, cancellando i dati su dischi accessibili in modo casuale e in blocchi da 64K, ha causato danni immediati senza rallentare significativamente la velocità di diffusione del worm.

Che cosa possiamo ricavare da tutto ciò? Di sicuro l'autore del worm è un programmatore esperto e intelligente; Witty è il primo worm a combinare un tale livello di bravura con un tale livello di malignità. O l'autore era già a conoscenza (magari dall'interno) della vulnerabilità (è improbabile che l'abbia ricavata tramite reverse-engineering dalla patch di ISS), oppure ha lavorato a gran velocità. Forse aveva il worm già pronto, ed ha aggiunto la vulnerabilità all'ultimo minuto. In ogni caso, pare che abbia voluto coscientemente prendere di mira la ISS. Se il suo obiettivo fosse stata la massima diffusione, avrebbe potuto attendere una vulnerabilità più generale, o una serie di vulnerabilità, da sfruttare. Quella da lui scelta era ottimizzata per infliggere il massimo danno ad uno specifico gruppo di bersagli. Si è trattato di un attacco contro ISS, o contro un particolare utente dei prodotti ISS? Non lo sappiamo.

Witty rappresenta un nuovo capitolo nel software maligno. Se per diffondersi avesse sfruttato delle comuni vulnerabilità di Windows, sarebbe stato il worm più dannoso mai visto prima. Gli autori di worm imparano dal lavoro di altri come loro, e dobbiamo presumere che altri autori di worm abbiano esaminato il codice disassemblato e che lo utilizzeranno per i prossimi worm. Ancora peggio, l'autore di Witty è tuttora sconosciuto e libero di agire -- e dobbiamo presumere che possa ripetere questo tipo di azioni.

< http://www.icsi.berkeley.edu/~nweaver/login_witty.txt >
< <http://www.securityfocus.com/printable/columnists/232> >

Questo intervento è originariamente apparso in Computerworld:

< <http://www.computerworld.com/securitytopics/security/virus/story/0,10801,93584,00.html> >
oppure < <http://tinyurl.com/ywvf2> >

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

Commenti dei lettori

Da: "Norman Bowley" <nbowley@e-counsel.ca>
Oggetto: RE: CRYPTO-GRAM del 15 maggio 2004

Una situazione simile a quella di Lacey è stata presa in esame una dozzina d'anni fa dalla Corte Suprema del Canada, con il caso James Henry Wise. Anche se l'ammissione delle prove ottenute grazie al dispositivo di tracciamento è stata approvata a stretto margine di maggioranza (4 favorevoli, 3 contrari), persino la maggioranza ha dichiarato che si era al limite della legalità. Il dissenso di La Forest, tuttavia, è inquietante e profetico: "Le conseguenze a lungo termine per l'integrità del nostro sistema giuridico, derivanti dall'ammissione di prove ottenute in tali circostanze, pesano molto di più del danno provocato dall'assolvimento dell'imputato. Questo non è un caso in cui le forze dell'ordine stanno controllando le strade allo scopo di regolamentare o di osservare quel che succede. Qui si tratta di tenere traccia dei movimenti di un individuo. Esiste un'importante differenza fra correre il rischio che le nostre attività possano essere osservate da altre persone e il rischio che agenti di stato, in mancanza di previa autorizzazione, possano tracciare ogni nostra mossa... La grave minaccia alla privacy individuale posta dal furtivo tracciamento elettronico dei movimenti di qualcuno è tale da richiedere una preliminare autorizzazione giudiziaria. L'emissione di un mandato di perquisizione richiederà solitamente una dimostrazione oggettiva di causa ragionevole e probabile, e questa dovrebbe essere la prassi necessaria per chiunque intenda impiegare dispositivi elettronici di tracciamento nella ricerca di un individuo".

Si può leggere la risoluzione qui:

< http://www.lexum.umontreal.ca/csc-scc/en/pub/1992/vol1/html/1992scr1_0527.html >
oppure < <http://tinyurl.com/2dzfb> >

Da: "Brian Gladman" <brg@gladman.plus.com>
Oggetto: La crittografia di WinZip

Il punto di vista secondo cui la morale che occorre imparare dai difetti presenti nella crittografia basata su AES di WinZip è che "la crittografia è materia difficile", potrebbe essere usato per indicare come questi difetti siano il risultato di errori commessi nel progetto di sicurezza utilizzato. Se si considera una problematica relativamente minore, credo che ciò possa essere vero.

Ma finora i punti deboli più significativi che sono stati trovati erano noti durante il processo di progettazione della sicurezza e sono stati mantenuti a causa del bisogno di compatibilità all'indietro. Ciò mi suggerisce una morale diversa (e di certo non nuova): aggiungere sicurezza ad un progetto già esistente come ripensamento difficilmente avrà successo.

Da: odlyzko@dtc.umn.edu (Andrew Odlyzko)

Oggetto: "solo i passeggeri muniti di biglietto sono ammessi ai controlli di sicurezza"

Due dei potenziali sviluppi per la sicurezza degli aeroporti che lei sostiene sono in un certo qual modo contraddittori. Avere degli "ufficiali della sicurezza in incognito [che] circolano all'interno [degli aeroporti]" -- cosa a lei gradita -- è molto più efficace se "solo i passeggeri muniti di biglietto sono ammessi ai controlli di sicurezza" -- cosa che invece secondo lei dovrebbe essere gradualmente eliminata. La restrizione ai passeggeri muniti di biglietto non solo serve ad accorciare le code ai controlli di sicurezza, ma riduce anche gli affollamenti all'interno, e semplifica il lavoro degli ufficiali di sicurezza in incognito.

Da: Christopher Bardin <christopher_b85281@yahoo.com>

Oggetto: Come trasformare una macchina fotografica usa-e-getta in una pistola paralizzante.

Riparo macchine fotografiche da più di 15 anni, e quindi sono forse più idoneo di un comune lettore a commentare l'articolo in oggetto. Pur non riparando macchine usa-e-getta (nessuno lo fa), ho avuto modo di smontarle per vedere che cosa contengono. E vi sono svariati errori madornali nella pagina web a cui fa riferimento l'articolo da lei indicato.

Anzitutto, non ho mai visto una macchina fotografica con un flash incorporato che avesse un condensatore da più di 350 Volt. Chiunque abbia inaspettatamente terminato un circuito da 350 Volt con una parte del proprio corpo potrebbe dissentire, ma ritengo che la differenza fra 350 e 600 Volt sia decisamente notevole -- anche se, di certo, 350 Volt non sono trascurabili.

In secondo luogo, una volta stabilito il rischio considerevole dei 350 Volt, è importante sapere che semplicemente togliendo la batteria dalla macchina non sarà sufficiente a far scaricare il condensatore del flash. Le macchinette fotografiche con flash incorporato non hanno resistenze di scarica lungo il condensatore del flash, perché non avrebbe senso. La resistenza di scarica dovrebbe essere di valore elevato (almeno 10 MegaOhm) per massimizzare la vita della batteria, e inoltre fisicamente grossa, dato il voltaggio necessario. Non è certo un componente a buon mercato. Dato che lo spazio è sopra la pari e il costo è sempre un problema, si sceglie sempre di non includerlo.

Da: Dan DeMaggio <dmag@umich.edu>

Oggetto: Passo 1: ammettere l'esistenza di un problema

Mi piacciono moltissimo la sua Crypto-Gram e le sue analisi ponderate. Ma devo rimproverarla per aver inserito il link all'articolo di Tim Mullen su Security Focus riguardante Walter Mossberg (e presumendo che lei sia dello stesso parere).

Tim dice: "La soluzione per l'utente finale è quella di incominciare a avere cura [di queste cose]". Ma ciò non accadrà mai. Solo i fanatici dei computer hanno cura dei computer. Solo i patiti di automobili hanno cura delle automobili. Solo gli appassionati dei lama hanno cura dei lama. Alla stragrande maggioranza della gente nel resto del mondo non importa un bel niente di queste cose.

Lasci che le parli di tre prodotti che ho acquistato:

- Ho comprato un'auto. Le serrature non sono un gran deterrente, ma hanno tenuto la mia auto perfettamente al sicuro (persino a Detroit) per più di 10 anni. La porto in officina dieci minuti ogni tre mesi per un cambio d'olio (come viene suggerito dal manuale d'uso e manutenzione). Quando si guasta (due volte in 10 anni), faccio una telefonata e me la riparano. Per me l'auto non è altro che un mezzo per raggiungere un fine. Non mi curo della mia auto.

- Ho comprato una casa. Mi aspetto che le serrature la mantengano ragionevolmente sicura. I complessi macchinari nel seminterrato possono rompersi ogni tanto, ma niente che non possa essere sistemato da una semplice visita di un tecnico riparatore. Ho molta più cura della mia casa

che non della mia auto, ma non più di tanto. Non avrei mai comprato la casa se questa fosse stata solo una costosa fonte di problemi.

- Ho preso a mia moglie un computer con installato Windows. Pochi istanti dopo averlo collegato aveva già cominciato a ricevere pop-up di spam. Se mi sbagliavo a scrivere un indirizzo Web, venivo dirottato su un sito che generava così tanti messaggi pop-up e moltiplicazioni di finestre che dovevo riavviare il computer. Mantenersi aggiornati scaricando le varie patch diventava un lavoro di diverse ore ogni mese. Anche se sono un amante della tecnologia, mi rifiuto di fare da baby-sitter a quel computer. Se si infetta, immagino che piatterò tutto e farò una reinstallazione pulita.

I primi due esempi sono "whole product", prodotti integrati (cfr. "Crossing the Chasm" di Geoffrey A. Moore). Quasi ogni cosa di cui avrei avuto bisogno è arrivata in bundle. Le cose non comprese erano elementi dei quali ero al corrente, cose assolutamente a poco prezzo (relativamente al prezzo del prodotto), e cose che non richiedono molto tempo o attenzione da parte mia.

Il terzo prodotto non è un prodotto integrato. Mi rifiuto di andare a caccia di tutti quei servizi che devo disattivare (ma ho preso un firewall, di sicuro). Mi rifiuto di sprecare il mio tempo a scaricare patch di svariati megabyte e attendere che il computer si riavvii innumerevoli volte. Mi rifiuto di spendere 100 dollari per proteggere un computer che ne vale 500, soprattutto perché non esiste software antivirus che mi protegge da tutti i nuovi exploit (lo so perché ricevo regolarmente dei virus tramite email che sono contrassegnate come "esenti da virus" dai rivenditori di antivirus).

Mi rifiuto di fare queste cose perché so che non devono essere fatte (e la maggior parte della gente non le farà comunque). Linux non ha bisogno di niente del genere. So che neanche Linux è un prodotto integrato (non ancora), ma è più semplice aggiungere documentazione e supporto a Linux piuttosto che sicurezza a Windows. Se io fossi veramente paranoico in materia di sicurezza, migrerei (facilmente) a OpenBSD. Ha avuto soltanto un buco remoto nell'installazione di default negli ultimi otto anni -- un po' diverso dai sette exploit in un giorno solo di Microsoft.

Walter dice: "È il momento che qualcuno [si faccia carico del fardello di proteggere i PC]". La gente vuole che i computer siano a basso mantenimento quanto un'automobile. Microsoft ha creato questo problema perché (in quanto monopolio), non è conveniente sistemare i bug (non porteranno aumenti delle vendite) o rendere le cose più sicure (come sopra). Certo, Tim, è una chimera sperare che il problema venga risolto gratis, ma è ancora più irrealistico aspettarsi che la gente si prenda cura dei computer.

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

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

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.

Inoltre 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> >.

Counterpane Internet Security, Inc. è leader mondiale nel monitoraggio guidato della sicurezza informatica. Gli analisti esperti in sicurezza di Counterpane proteggono reti per aziende inserite nella Fortune 1000 a livello mondiale.

Copyright (c) 2004 by Bruce Schneier.