

CRYPTO-GRAM
15 novembre 2003

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.

** **

In questo numero:

[Gli hacker degli aerei](#)
[La vera arma dei terroristi dell'11 settembre 2001](#)
[Le ristampe di Crypto-Gram](#)
[News](#)
[Le News di Counterpane](#)
[Altre recensioni di "Beyond Fear"](#)
[Il Canile: SunnComm Technologies](#)
[La difesa del Trojan](#)
[Commenti dei lettori](#)

** **

Gli hacker degli aerei

Nathaniel Heatwole è uno studente del Guilford College. Per diverse volte, fra il 7 febbraio e il 15 settembre, si è cimentato nel collaudo della sicurezza delle linee aeree. Dapprima ha introdotto di nascosto taglierini, argilla per simulare esplosivi al plastico, e candeggina per simulare materiali chimici per realizzare bombe. Poi ha nascosto questi oggetti nelle toilette degli aerei, insieme ad alcune note. Infine ha inviato un messaggio e-mail alla TSA (Transportation Security Administration) intitolato "Informazioni riguardanti 6 recenti falle di sicurezza".

Il problema è che la TSA non gli ha mai chiesto di collaudare tale sicurezza.

Per anni, le reti informatiche sono state perseguitate da hacker che si introducono nei sistemi. Queste persone non penetrano nei sistemi a scopo di lucro. Non commettono frodi. Non rubano nulla. Si intrufolano nei sistemi per curiosità intellettuale. Per divertimento. Per mettersi alla prova, per vedere se ci riusciranno.

Una difesa tradizionale e molto usata da parte degli hacker è quella secondo cui loro si introducono nelle macchine per valutarne la sicurezza. Il concetto di fondo è che l'unico modo per apprendere la sicurezza informatica e delle reti sia quello di attaccare i sistemi. Non importa se questi hacker non possiedono i sistemi in cui irrompono; quella è la scusa.

Il Dipartimento della Sicurezza Nazionale e la Transportation Security Administration sono stati attaccati dal loro primo hacker. Non si è trattato di un terrorista; né di qualcuno intenzionato a dirottare aerei. Non si è trattato neanche di un criminale; non ha infatti cercato di estorcere

denaro. È stato un hacker, puro e semplice. Ha voluto mettere alla prova l'efficacia dei controlli di sicurezza. Ha voluto dimostrare che le misure di sicurezza erano -- ai suoi occhi -- quantomeno inadeguate. Ha voluto aggirare la sicurezza degli aeroporti.

Punto primo: tutto ciò è incredibilmente sciocco. Ogni viaggiatore di mia conoscenza può riportare innumerevoli storie di coltelli che non sono stati individuati dalla sicurezza in aeroporto. Nessuno che viaggi in aereo con regolarità ritiene che la TSA stia facendo un buon lavoro nell'impedire la presenza di oggetti affilati a bordo. Ancora peggio, nessuno che viaggi in aereo con regolarità ritiene che impedire la presenza di oggetti affilati a bordo ci renda tutti più sicuri. Molto di quel che la TSA svolge è una messinscena, un qualcosa che dia l'idea di sicurezza. Mantiene le apparenze, e forse (si spera) fa in modo che eventuali terroristi non siano così tanto sicuri di poter introdurre armi a bordo di un aereo. Probabilmente no.

Punto secondo: questo è un reato, e dovrebbe essere trattato come tale. "Stavo solo verificando la sicurezza" non è una valida difesa. Noi che lavoriamo nell'ambito della sicurezza informatica abbiamo sentito questa scusa per anni. Siccome l'hacker non intendeva arrecare danni, siccome ha penetrato il sistema solo per dare un'occhiata qua e là, non si è trattato di un vero crimine. Facciamo un esempio: voi rientrate a casa vostra e trovate questo biglietto attaccato sul frigorifero: "Stavo verificando la sicurezza delle porte di servizio di tutto il vicinato e ho notato che la sua non era chiusa a chiave. Ho soltanto dato un'occhiata in giro. Non le ho rubato nulla. Dovrebbe far sistemare la sua serratura". Non vi sentireste violati? Naturalmente sì.

Punto terzo: si tratta di certo di un reato, ma non di un reato estremamente grave. La bravata di Heatwole è stata imbarazzante, e le indagini e il lavoro di "ripulitura" sono costati parecchio denaro. Avrebbe potuto compromettere i programmi di viaggio di molte persone. Ma il ragazzo non è un terrorista. Non ha agito per passare ad al Qaeda informazioni sulla sicurezza. Le sue azioni non hanno messo a rischio la vita di nessuno. Gli si vorrebbe infliggere una severa punizione, poiché ha gettato nell'imbarazzo importanti funzionari del governo, ma questa non è una ragione sufficientemente valida. Da una parte si deve scoraggiare questo tipo di comportamento, dall'altra occorre che la punizione sia commisurata al reato. Si tratti Heatwole come un criminale, ma non come un criminale pericoloso.

Benvenuto nel nostro mondo, Dipartimento della Sicurezza Nazionale. Benvenuta, TSA. Abbiamo combattuto per anni contro questo genere di individui. Forse perseguendoli avrete più fortuna, ma non lasciate che la rabbia prevalga sulla razionalità.

Una versione di questo articolo è apparsa su IEEE Security & Privacy
<<http://www.computer.org/security/>>

News:

<<http://www.cnn.com/2003/US/10/18/airline.scare/index.html>>

<<http://www.nytimes.com/aponline/national/AP-Planes-Searched.html>>

<http://www.salon.com/news/wire/2003/10/20/box_cutters2/>

Altri interventi:

<<http://www.securityfocus.com/columnists/194>>

<http://www.salon.com/tech/col/smith/2003/11/07/askthepilot63/index_np.html>

Un altro taglierino è stato trovato su un aereo. Nessuno sa chi possa averlo lasciato.

<<http://www.cnn.com/2003/US/10/28/airline.boxcutter/index.html>>

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

La vera arma dei terroristi dell'11 settembre 2001

Un buon pezzo su @Stake e sull'integrità delle loro azioni nel licenziare Dan Geer:
<<http://www.eweek.com/article2/0,4149,1335621,00.asp>>

Il verdetto di colpevolezza per un uomo in California accusato di hacking è stato rivisto in appello. È incredibile quanto accaduto, specie considerando il fatto che questa persona ha passato in carcere più di un anno. Una vittoria per i "buoni", indubbiamente, ma ci è voluto troppo tempo.

<<http://news.com.com/2100-7348-5092697.html>>
<<http://www.securityfocus.com/news/7202>>

"Identità ed Economia": la presentazione dal DefCon.
<<http://www.homeport.org/~adam/shostack-bh-vegas-03-final.ppt>>

Un manuale di operazioni terroristiche, che si crede sia stato usato da al Qaeda:
<<http://www.thesmokinggun.com/archive/jihadmanual.html>>

Alcune parti interessanti: le comunicazioni consigliate sono quasi tutte low-tech. Nessun supporto per tutte quelle speculazioni riguardanti la steganografia. I codici e i cifrari consigliati sono sistemi manuali molto semplici. Probabilmente non si tratta di sicurezza ad alti livelli.

Si scopre che molte automobili hanno dei passe-partout che vengono utilizzati dai malviventi per rubare macchine.
<<http://www.philly.com/mld/inquirer/classifieds/automotive/6876246.htm>>

Un interessante articolo sulla sicurezza dei casinò. (Si faccia molta attenzione a prendere per oro colato i dettagli di articoli come questo. Molte di queste storie vengono messe in circolazione dagli stessi casinò per convincere il pubblico della bontà della loro sicurezza nel rilevare gli imbrogli. In realtà tale sicurezza non è così efficace).
<<http://www.csoonline.com/read/100103/kind.html>>

Intercettare le comunicazioni fra terroristi. Il problema non è la raccolta dei dati, ma la loro analisi:
<<http://www.msnbc.com/news/982235.asp?cp1=1>>

Le vulnerabilità della sicurezza informatica: la Top 20 del SANS:
<<http://www.sans.org/top20/>>

La California security-breach disclosure law sembra non aver sortito alcun effetto:
<<http://www.securityfocus.com/news/7311>>

Un'eccellente analisi della sicurezza di Windows confrontata con quella di Linux:
<<http://www.groklaw.net/article.php?story=20031022014413296>>

Pare che molti codici delle patenti di guida statunitensi non siano affatto casuali, ma che contengano informazioni sul vostro nome, cognome, ecc. Questo è un sito interessante che tratta appunto tali codici. Una lettura fondamentale se siete intenzionati a creare un ID fasullo.
<<http://www.highprogrammer.com/alan/numbers/>>

Bruce Tognazzini sulle interfacce di sicurezza informatica:
<<http://www.asktog.com/columns/058SecurityD'ohIts.html>>

L'Australia sembra intenzionata ad implementare il voto elettronico in maniera appropriata:
<<http://www.wired.com/news/ebiz/0,1272,61045,00.html>>

Nuovi rischi per la privacy. In Pakistan, un'impiegata addetta alle trascrizioni mediche (attraverso tre livelli di subappaltatori) ha minacciato di rendere pubbliche su Internet diverse

<<http://www.forbes.com/markets/newswire/2003/10/27/rtr1124430.html>>
<http://news.com.com/2102-7349_3-5092781.html>
<<http://news.bbc.co.uk/1/hi/technology/3202116.stm>>
<<http://www.theregister.co.uk/content/55/33460.html>>
<<http://www.theregister.co.uk/content/55/33636.html>>

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

Commenti dei lettori

Da: Russell Nelson <nelson@crynwr.com>
Oggetto: Re: I copricapi nelle banche

> Una volta è stato chiesto a un detective di New York se i borseggiatori a Manhattan si
> vestissero in giacca e cravatta per non attirare attenzione, portare a termine più facilmente i
> loro colpi e scappare. Egli ha risposto che in vent'anni non aveva mai arrestato un
> borseggiatore in giacca e cravatta.

Ma questo viene portato come prova per sostenere la sua opinione o per confutarla? Perché a me sembra che se quel detective non ha mai arrestato un borseggiatore in giacca e cravatta, questa è un'ottima prova per sostenere che i borseggiatori in giacca e cravatta riescono a farla franca.

Da: Troy Davis <troy@nack.net>
Oggetto: Furto di identità e Conti Capitali online

> Un 19enne si è servito di un finto sito Web per indurre i malcapitati a scaricare il suo
> software (un cavallo di Troia) e poi si è impadronito delle informazioni sui loro conti capitali
> e ha investito in borsa usando i loro nomi.
> [...] La cosa allarmante è la potenziale efficacia di questo attacco. Questo ragazzo era
> stupido e ingenuo, ma immaginiamo per un istante quali risultati si avrebbero se un
> aggressore più scaltro pianificasse meglio un attacco del genere. Potrebbe diventare
> milionario e lasciare il paese prima che qualcuno se ne accorga.

Malgrado chi ha un conto capitale online sia un facile bersaglio, si può fare di tutto e di più ai danni dei clienti di banche più tradizionali che hanno abilitato l'accesso Internet ad un conto per fare trading online. L'abilitazione di un conto spesso permette in automatico di effettuare transazioni online per tutti i conti aperti sulla stessa banca, attraverso la medesima password.

Come risultato, il pieno accesso via Internet a tutti i conti bancari è spaventosamente diffuso anche fra gli utenti occasionali. Al signor Pinco Pallino serve avere la possibilità di spostare 50.000 dollari senza una telefonata né tantomeno una visita alla banca? Non solo non mi occorre questa possibilità, non la voglio nemmeno.

I più esperti non si scomoderebbero neanche ad usare dei Trojan. Basta scegliere dei professionisti in carriera o la cui carriera è ormai consolidata, con salari sostanziosi, una esperienza informatica di base e altri fattori verificabili associati ad un uso attivo di Internet (ragazzi in età scolare, professioni che richiedono il telelavoro, ecc.).

Prendiamo uno dei tanti metodi assolutamente legittimi di accesso fisico ai sistemi: l'impresa di pulizie di un ufficio legale, o il personale addetto alla manutenzione di un palazzo nel centro città. Recuperate i log di tastiera qualche settimana dopo.

Come lei dice, l'attaccante sarebbe già fuori dal paese o fuori dal raggio d'azione di un radar (open WAP) non solo prima che qualcuno se ne accorgesse, ma ancora prima dell'inizio della prima transazione. L'equivalente online dei limiti di velocità delle transazioni di un bancomat --

dopo tre prelievi da 300 dollari ciascuno, la carta viene bloccata -- avviene molto più raramente di quanto si sia portati a credere.

Da: Ton van der Putte <Ton.vanderPutte@atosorigin.com>
Oggetto: Ingannare i rilevatori di impronte digitali

Nel numero di CRYPTO-GRAM di giugno 2002, lei ha fatto riferimento al nostro articolo "Don't get your finger burned" [Non scottatevi le dita]. In quell'articolo descriviamo due metodi per duplicare le impronte digitali. Un metodo presuppone la collaborazione di qualcun altro (disposto a "prestare" il proprio dito per la creazione del duplicato), mentre con il secondo metodo un'impronta latente, dopo essere stata asportata, viene duplicata tramite un processo fotochimico. Con queste impronte fasulle siamo stati in grado di ingannare ogni sensore di impronte testato nel nostro laboratorio e in ogni dimostrazione pubblica (con rilevatori di circa 20 marche diverse). Ho iniziato con questi esperimenti nei primi anni novanta, cioè più di dieci anni fa.

La scorsa settimana siamo stati invitati dalla BBC a raggiungere Londra per un'intervista sulla duplicazione delle impronte digitali. Questo perché l'Amministrazione Britannica intende aggiungere degli elementi biometrici alle nuove carte d'identità inglesi, e una delle opzioni riguarda appunto le impronte digitali. Il programma, "Kenyon Confronts" è stato mandato in onda mercoledì 29 ottobre, e può essere visionato online (per un periodo limitato) sul sito Web della BBC.

Dato che i miei esperimenti risalivano a dieci anni prima, decisi di rifarli. Sapevo che sarebbe stato ancora più facile duplicare impronte con tutti i materiali e le attrezzature disponibili oggi, ma i risultati mi hanno comunque stupito. Per darle un'idea: dieci anni fa, per realizzare il duplicato di un'impronta digitale mediante cooperazione mi ci volevano dalle due alle tre ore, e per un risultato ottimale mi ero servito di materiali utilizzati dagli odontotecnici. Oggi posso usare materiali acquistabili in un qualsiasi negozio di fai-da-te, per un costo complessivo di circa dieci dollari (e che sono sufficienti per circa 20 dita fasulle).

Il tempo necessario a creare un duplicato perfetto è ora di circa 15 minuti (con del materiale specifico si può ridurre a 10 minuti). Per creare il duplicato di un'impronta rilevata mi occorsero parecchi giorni nel 1992, e furono necessari parecchi esperimenti prima di trovare il procedimento e la tecnica adeguati. Adesso mi basta mezz'ora e i costi dei materiali si aggirano sui 20 dollari (anche in questo caso sono sufficienti a creare circa 20 duplicati); le uniche attrezzature necessarie sono una fotocamera e una lampada a raggi UV. Non solo ora posso realizzare i duplicati in una frazione del tempo che mi sarebbe servito in precedenza, ma anche la qualità è migliore.

La ragione per cui le scrivo tutto questo è la seguente: sebbene molti produttori di rilevatori di impronte continuano a ignorare che esiste un problema, oppure dichiarino di averlo risolto, altri sono propensi ad ammetterlo, però sostengono che sia molto difficile e costoso riprodurre le impronte digitali, e che può essere fatto solo da professionisti molto capaci. Innanzitutto penso che non si tratti di un'argomentazione molto convincente, e in secondo luogo ammetto di essere un professionista, ma ora un qualsiasi hobbista è in grado di ottenere dei buoni risultati, ed è una tecnica che non richiede mezzi o abilità particolari.

È perciò nostra opinione che, finché i costruttori di attrezzature per il rilevamento delle impronte non risolveranno il problema del rilevamento dal vivo (cioè il poter distinguere fra un dito vero e proprio e un duplicato fasullo), i sensori biometrici delle impronte digitali non dovrebbero essere utilizzati in combinazione alle carte d'identità o in quelle applicazioni di media e alta sicurezza. Infatti riteniamo inoltre che documenti di identità dotati di tali sensori biometrici siano ancor meno sicuri dei documenti che ne sono privi. I due esempi che seguono possono chiarire quanto affermiamo.

