

CRYPTO-GRAM
15 agosto 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:

“BOB” a bordo
Gli alibi e la gentilezza degli sconosciuti
Le ristampe di Crypto-Gram
News
Note di sicurezza da ogni dove: il GHB
Le News di Counterpane
I ranger dell'aeroporto di Houston
Siti Web, password e consumatori
Commenti dei lettori

** **

“BOB” a bordo

L'allarme bomba dello scorso martedì comprende qualche interessante lezione di sicurezza, insieme buona e cattiva, su come raggiungere la sicurezza in questi tempi sempre più pericolosi. Novanta minuti dopo aver lasciato l'aeroporto di Sydney, uno steward di un volo della United Airlines diretto a Los Angeles ha trovato un sacchetto per il mal d'aria (presumibilmente non usato) in una toilette. Sul sacchetto erano scritte le lettere “BOB”. Lo steward ha stabilito che le tre lettere stavano per “Bomb On Board” (bomba a bordo) e ha immediatamente avvertito il comandante, il quale ha deciso che il rischio era sufficientemente alto da interrompere il volo e tornare indietro all'aeroporto di Sydney.

Basta ragionare un poco per rendersi conto di come questa sia una reazione esagerata di fronte a una minaccia inesistente. “Bob” è un'espressione gergale molto comune fra il personale di volo, e sta per “babe on board” o “best on board”, cioè “bello/a a bordo” (ad esempio: “Guarda quella Bob al posto 7A”). La United Airlines pare che si serva della stessa abbreviazione in alcuni voli interni agli USA per indicare “Buy on Board”, cioè “acquista a bordo”: i pasti non vengono offerti gratuitamente, perciò, se lo si desidera, occorre pagare. Inoltre, anche se poco probabile, non è nemmeno scartabile l'ipotesi che “BOB” sia semplicemente il nome di qualcuno, scritto sul sacchetto per il mal d'aria tempo prima e dimenticato nella toilette accidentalmente da qualche passeggero. Perché diamine qualcuno, fra tutte le interpretazioni possibili della scritta “BOB” su un sacchetto per il mal d'aria, deve stabilire a priori che la presenza di quel particolare sacchetto sul quel particolare volo non possa voler dire altro che “bomba a bordo”?

E perché il comandante dovrebbe essere d'accordo?

La sicurezza funziona al meglio quando le persone sono direttamente incaricate. Mi conforta il fatto che la decisione finale di interrompere e deviare il volo sia stata presa dal comandante del volo e non da qualche quadro della United Airlines che avrebbe potuto preoccuparsi, più che della minaccia, dei centomila dollari che l'atterraggio di emergenza sono venuti a costare. Il comandante ha la responsabilità dell'aereo, ed è la figura migliore per bilanciare da una parte il rischio per le vite dei passeggeri (e la propria), e dall'altra la seccatura comportata dalla deviazione del volo.

Sempre più spesso i nostri sistemi di sicurezza sono gestiti da computer e da linee di condotta inalterabili, che trasformano in robot le persone che stanno in prima linea per quanto riguarda la sicurezza. Ora sono i computer a scegliere chi ispezionare accuratamente ai checkpoint negli aeroporti. Alle reception, guardie esperte sono state rimpiazzate da impiegati meno abili che controllano meccanicamente i documenti di identità. Questa storia serve da controesempio, e dimostra la maniera corretta per progettare un sistema di sicurezza.

Tuttavia, se ci dobbiamo aspettare che i comandanti e il personale di volo prendano importanti decisioni di sicurezza, allora è necessario addestrare queste persone. Lo steward che ha trovato il sacchetto per il mal d'aria non ha reagito seguendo il razio cinio, ma la paura. E quella paura ha contagiato anche il comandante, che ha preso una decisione sbagliata.

La paura non renderà nessuno più sicuro. Provoca solo reazioni esagerate di fronte a falsi allarmi. Ci invita a spendere cifre sempre più alte e a rinunciare a un sempre maggior numero di libertà civili, senza ricevere alcuna sicurezza in cambio. Ci rende ciechi alle vere minacce.

Parlando della persona che ha scritto quelle tre fatali lettere sul sacchetto per il mal d'aria, il Ministro dei Trasporti John Anderson lo ha definito "quantomeno irresponsabile, per non dire tremendamente egoista e stupido". Irresponsabile per aver fatto cosa? Per aver scritto il proprio nome? Per aver utilizzato un comunissimo gergo da personale di volo? Non è stato chi ha scritto a far qualcosa di sbagliato, ma chi ha reagito di fronte alla scritta.

Viviamo in tempi spaventosi, ed è facile che la paura prenda il sopravvento sulla nostra capacità di ragionare. Ma proprio perché si tratta di tempi spaventosi è importante evitare che ciò accada. Il Primo Ministro John Howard ha lodato l'equipaggio per rapidità di riflessi, diligenza e capacità di osservazione. Spiacente, ma non vedo alcuna prova di tutto questo. Tutto quel che vedo sono persone che sono state spinte a rivestire un importante ruolo di sicurezza reagendo in base alla paura, perché non sono state debitamente addestrate a valutare razionalmente le situazioni di sicurezza: i rischi, le contromisure, e i compromessi. Ci fossero state menti più calme e razionali in cabina, questa storia avrebbe avuto un esito ben diverso.

Purtroppo la paura genera altra paura, e produce un clima in cui finiamo col terrorizzare noi stessi. Adesso qualsiasi pazzoide nel mondo sa che gli basta scrivere "BOB" su un sacchetto per il mal d'aria per impedire il decollo di un volo internazionale. Non credo sia questo il risultato che volevamo.

< <http://www.foxnews.com/story/0,2933,127109,00.html> >

< http://www.heraldsun.news.com.au/common/story_page/0,5478,10269885^1702,00.html >

oppure < <http://tinyurl.com/4momw> >

Questo articolo è apparso originariamente sul Sydney Morning Herald:

< <http://www.smh.com.au/articles/2004/08/02/1091298614078.html> >

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

<<http://www.schneier.com/crypto-gram.html>>. Quella che segue è una selezione di articoli apparsi in questo mese gli anni scorsi.

Volare con un biglietto aereo altrui:

<<http://www.schneier.com/crypto-gram-0308.html#6>> (versione originale)

<<http://www.cryptogram.it/agosto03.htm#a6>> (traduzione in italiano)

Il testo nascosto nei documenti elettronici:

<<http://www.cryptogram.it/agosto03.htm#a8>> (versione originale)

<<http://www.schneier.com/crypto-gram-0308.html#8>> (traduzione in italiano)

Palladium e il TCPA:

<<http://www.schneier.com/crypto-gram-0208.html#1>> (versione originale)

<<http://www.cryptogram.it/agosto02.htm#a1>> (traduzione in italiano)

Armare i piloti delle linee aeree:

<<http://www.schneier.com/crypto-gram-0208.html#8>> (versione originale)

<<http://www.cryptogram.it/agosto02.htm#a8>> (traduzione in italiano)

Code Red:

<<http://www.schneier.com/crypto-gram-0108.html#1>>

La protezione del copyright nel Mondo Digitale:

<<http://www.schneier.com/crypto-gram-0108.html#7>>

Vulnerabilità, divulgazione e risoluzioni basate su virus:

<<http://www.schneier.com/crypto-gram-0008.html#2>>

Bluetooth:

<<http://www.schneier.com/crypto-gram-0008.html#8>>

Un "cracker" hardware DES:

<<http://www.schneier.com/crypto-gram-9808.html#descracker>>

Sistemi biometrici: Verità e Finzioni:

<<http://www.schneier.com/crypto-gram-9808.html#biometrics>>

Back Orifice 2000:

<<http://www.schneier.com/crypto-gram-9908.html#BackOrifice2000>>

Servizi e-mail basati sul Web e crittografati:

<<http://www.schneier.com/crypto-gram-9908.html#Web-BasedEncryptedE-Mail>>

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

News

Il mese scorso ho pubblicato un link ad un paio di articoli di Salon sulla tortura. Questo articolo (dall'Atlantic dell'ottobre 2003) è ancora migliore: più intelligente, più equilibrato, più basato sui fatti... insomma, più sostanzioso. Inoltre, è stato scritto prima che qualsiasi dettaglio su Abu Ghraib arrivasse al grande pubblico.

<<http://www.theatlantic.com/issues/2003/10/bowden.htm>>

Se può sembrare che io spenda così tanto tempo parlando di sicurezza stupida, è perché mi capita molto raramente di vedere della sicurezza intelligente e questa è sicurezza intelligente. Alla VISA si

sono seduti e hanno ideato alcuni standard di progettazione rigorosi, ma ben ponderati, per quanto riguarda i dispositivi di inserimento PIN degli sportelli automatici delle banche. L'analisi comprende calcoli specifici degli sforzi che un aggressore deve compiere per sconfiggere tali dispositivi. Mi piace pensare che abbiano fatto tutto questo perché hanno letto i miei libri... Ma non posso esserne certo.

<http://www.theregister.co.uk/2004/07/21/atm_keypad_security/>

Nuove sanzioni penali negli Stati Uniti per il furto d'identità:

<http://news.com.com/Season+over+for+%27phishing%27%3F/2100-1028_3-5270077.html>
oppure <<http://tinyurl.com/6xhxx>>

Un gruppo di hacker sta vendendo del codice sorgente riservato:

<http://news.com.com/Psst-+wanna+buy+some+source+code%3F/2100-7355_3-5269787.html> oppure <<http://tinyurl.com/6md5q>>

Per esempio, il codice Enterasys per il rilevamento delle intrusioni costa 16.000 dollari:

<<http://www.eweek.com/article2/0,1759,1623182,00.asp>>

Anzi no; la società ha chiuso i battenti per conto suo:

<<http://www.computerworld.com/newsletter/0,4902,94552,00.html?nlid=SEC2>>

O meglio... sì: eccoli di nuovo al lavoro:

<http://www.infoworld.com/article/04/07/19/HNstolencodeshopback_1.html>

Ecco l'ennesimo articolo che dimostra come le aziende siano molto preoccupate della sicurezza:

<<http://www.vnunet.com/news/1156671>>

Non è interessante come tali preoccupazioni sembrano non tradursi mai in budget?

Il Ministro della Giustizia del Messico si è fatto impiantare un microchip RFID nel suo braccio. È progettato sia per fungere da dispositivo di verifica di accesso, sia per tenere traccia degli spostamenti del Ministro in caso di sequestro.

<<http://www.wired.com/news/technology/0,1282,64194,00.html>>

<http://quote.bloomberg.com/apps/news?pid=10000086&sid=aYyZfaVRFtWQ&refer=latin_america> oppure <<http://tinyurl.com/6sg68>>

<<http://www.fortune.com/fortune/print/0,15935,675442,00.html>>

Quel che è strano in questa storia, almeno per me, è il fatto che il chip sia progettato come "non-rimuovibile" e come questa funzionalità possa essere d'aiuto in caso di un sequestro. Magari sono il solo a pensarla così, ma ritengo che un criminale che abbia il valore e le capacità tali da rapire il Ministro della Giustizia del Messico, non si faccia molti problemi ad amputargli il braccio. Questo è un tipo di misura di sicurezza che si rivela più efficace mantenendola segreta.

Qui si parla di un'interessante vulnerabilità hardware di sicurezza. Pare che sia possibile aggiornare il microcodice del processore AMD K8 (Athlon64 o Opteron) e, udite udite, non c'è alcun controllo di autenticazione. Per cui è possibile che un aggressore che ha accesso diretto a una macchina possa creare una backdoor nella CPU.

<<http://www.realworldtech.com/forums/index.cfm?action=detail&PostNum=2527&Thread=1&entryID=35446&roomID=11>> oppure <<http://tinyurl.com/43kod>>

Un altro articolo di metrica finanziaria per giustificare le spese per la sicurezza informatica:

<<http://www.computerworld.com/newsletter/0,4902,94524,00.html?nlid=SEC2>>

Errori più frequenti riguardanti la sicurezza della posta elettronica:

<<http://www.computerworld.com/softwaretopics/software/story/0,10801,94507,00.html>>

oppure <<http://tinyurl.com/5zujx>>

Esiste un bilanciamento fondamentale fra la sicurezza e la compatibilità. Si può sistemare un'applicazione per renderla sicura, ma spesso così facendo si interrompe la compatibilità all'indietro. Microsoft, con XP SP2, ha scelto di sacrificare la compatibilità all'indietro puntando invece sulla sicurezza, e molti rivenditori sono infuriati. Io credo che Microsoft abbia preso una giusta decisione.

<<http://www.eweek.com/article2/0,1759,1624962,00.asp>>
<<http://www.informationweek.com/story/showArticle.jhtml?articleID=23902063>> oppure
<<http://tinyurl.com/6tmtz>>

Il Governo degli Stati Uniti sta ufficialmente ritirando il DES dagli standard crittografici:
<<http://csrc.nist.gov/Federal-register/July26-2004-FR-DES-Notice.pdf>>

Come rendere un cellulare un dispositivo di ascolto: "Oggi una qualsiasi Mata Hari da sala riunioni può comprare un modello particolare di telefono cellulare progettato per rispondere alle chiamate in arrivo pur sembrando spento. In un incontro d'affari, con la scusa di assentarsi qualche istante per andare al bagno, lei potrebbe lasciare casualmente sul tavolo il proprio telefonino. Una volta uscita dalla stanza potrebbe chiamare il telefono lasciato sul tavolo e ascoltare che cosa dice la controparte in sua assenza". Non riesco a trovare nulla che corrobora questa fonte, e mi farebbe piacere ricevere qualche indizio a riguardo.
<<http://slate.msn.com/id/2092059/>>

Ad ogni modo, se una cosa come questa vi preoccupa, o se volete pranzare in tutta tranquillità in un ristorante, potete sempre acquistare un jammer per cellulari. Si noti che questi dispositivi sono illegali negli Stati Uniti, anche se è possibile comprare degli aggeggi che deviano le frequenze dei telefonini statunitensi.
<<http://www.globalgadgetuk.com/cell%20phone%20jammers.htm>>

Dilbert, gli ufficiali di sicurezza, e i documenti d'identità con fototessera:
<<http://www.comics.com/comics/dilbert/archive/dilbert-20040801.html>>

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.
< <http://fob.webhop.net/> >

Secondo il loro sito Web, "la Central Intelligence Agency (CIA) si impegna a proteggere la vostra privacy e non raccoglierà informazioni personali su di voi a meno che non siate voi a fornirci tali informazioni". Hmm, ma non è il loro mestiere quello di raccogliere informazioni personali senza chiedere il permesso agli interessati?
<<http://www.odci.gov/cia/notices.html#priv>>

Una truffa per riciclare denaro via e-mail. Registrate un conto presso i truffatori, ed essi iniziano a trasferirvi denaro rubato da altri conti. Il vostro compito è trasferire il denaro verso i truffatori attraverso percorsi non tracciabili, e come ricompensa vi tenete una percentuale. Per lo meno, ve la tenete finché i possessori dei conti violati non si accorgeranno che sono stati trasferiti dei soldi sul vostro conto senza il loro permesso. Poi l'FBI verrà a bussarvi alla porta.
<<http://www.codephish.info/modules.php?op=modload&name=News&file=index&catid=&topic=5>> oppure <<http://tinyurl.com/5q79p>>

Pare che le banche stiano facendo del loro meglio per non dover rimborsare i clienti vittime di attacchi "phishing".
<<http://business.bostonherald.com/financeNews/view.bg?articleid=36056>>
Non dovrebbe essere difficile risolvere la questione. Sì, è colpa dei clienti se sono caduti nella trappola dei truffatori. Ma sono le banche, in primo luogo, ad aver realizzato dei sistemi di sicurezza facilmente aggirabili, ed è compito delle banche far fronte al problema. Così come il governo statunitense ha limitato a 50 dollari la responsabilità personale per una carta di credito rubata, dovrebbero fare una cosa del genere con i conti via Internet.

Gli effetti dei lampioni stradali sulla sicurezza. Ovviamente, questo sito Web è a favore dell'astronomia e contro l'inquinamento da eccessiva illuminazione, ma è interessante notare come l'aumento dell'illuminazione non influisca sui tassi di criminalità.
<<http://www.dark-skies.org/theproblems.html#security>>

Ancora sull'hacking del protocollo Bluetooth. Si discute di un dispositivo chiamato "fucile BlueSniper", cioè in pratica un'antenna direzionale. È un dispositivo proof- of- concept, ma pare che qualcuno, armato di questo "fucile", si sia appostato fuori da un albergo, abbia mirato ad una finestra dell'undicesimo piano, e abbia raccolto 300 rubriche telefoniche intercettando vari dispositivi Bluetooth. Ha anche battuto ogni record di distanza, attaccando un telefonino Nokia 6310i a più di 1.1 miglia e ricavandone la rubrica telefonica e i messaggi di testo.

<<http://www.wired.com/news/privacy/0,1848,64463,00.html>>

Qualcuno ha costruito uno strumento di packet injection per reti wireless 802.11. Con esso è possibile inserirsi nella connessione Internet wireless di qualcun altro e modificarne i pacchetti: falsificare e-mail, pagine Web, qualsiasi cosa. Pensateci un momento: chiunque potrebbe fare una gran quantità di danni con uno strumento simile.

<<http://www.evilscheme.org/defcon/>>

C'è una interessante strategia di difesa contro il furto d'identità. Si chiama "security freeze" e permette ai singoli individui di bloccare gli accessi ai documenti di credito fino a quando loro stessi non sbloccheranno i file relativi contattando personalmente le agenzie di credito e fornendo un codice PIN. Naturalmente le associazioni di credito stanno bloccando questa procedura: per loro si tratta di un aumento di lavoro, e non si accollano i costi di un furto d'identità. Questo è un ottimo esempio di organizzazione che impedisce una soluzione di sicurezza perché non mostra di essere finanziariamente interessata al problema.

<<http://www.cnn.com/2004/TECH/biztech/08/03/security.freeze.ap/>>

C'è un nuovo sito Web che ruba password tramite "phishing", ed è mascherata da sito di propaganda per l'elezione a presidente di John Kerry:

<<http://www.computerworld.com/securitytopics/security/cybercrime/story/0,10801,95030,00.html>> oppure <<http://tinyurl.com/67qo9>>

<<http://www.eweek.com/article2/0,1759,1630161,00.asp>>

Bush e Kerry si trovavano nella medesima cittadina nello Iowa. L'avvenimento ha tenuto occupate le forze di polizia al massimo, e alcuni rapinatori di banche ne hanno approfittato: tre banche sono state derubate nel corso della giornata.

<<http://news.bbc.co.uk/1/hi/world/americas/3533478.stm>>

Una cosa del genere è accaduta anche in un episodio dei Simpsons, intitolato "Marge contro la monorotaia", in cui alcuni rapinatori svaligiano diverse abitazioni mentre i cittadini sono tutti riuniti a una manifestazione cittadina.

È un sito scherzoso, e val la pena farci un giro:

<<http://www.preparingforemergencies.co.uk/>>

Il paragrafo introduttivo della notizia dice: "Cinque container di limoni sono marciti dopo che la nave su cui erano caricati è stata trattenuta al largo di New York per una settimana. Gli ufficiali avevano ricevuto una falsa soffiata dalla sicurezza, secondo cui il carico poteva essere biologicamente contaminato...". Questo è per me spunto di interessanti riflessioni. In quali modi delle persone senza scrupoli possono servirsi del terrorismo anonimo per gettare scompiglio fra le aziende concorrenti o semplicemente per danneggiare deliberatamente certe compagnie?

<<http://www.reuters.com/newsArticle.jhtml?type=oddlyEnoughNews&storyID=5911191&src=rss/oddlyEnoughNews§ion=news>> oppure <<http://tinyurl.com/4ra4r>>

Questo hard disk USB/Firewire portatile sembra proprio bello. Tutti i dati vengono automaticamente criptati quando sono archiviati sul disco, e decodificati quando sono trasferiti dal disco. Possiede una chiave fisica che racchiude la chiave di cifratura, e senza di essa i dati sono inaccessibili. Con tutto questo ben di dio, e con il fatto che la crittografia è triple-DES, perché diamine hanno limitato la chiave a 64 bit? Una chiave più lunga non è affatto più lenta. L'esportazione non è più un problema. Che peccato, davvero.

<<http://www.thinkgeek.com/gadgets/security/68b7/>>

L'evento raro e spettacolare sembra sempre più pericoloso di una cosa comune e banale, e a causa di ciò finiamo col subire molte messinscene di sicurezza.

<<http://www.englishmajor.com/rapefacts.html>>

Vi sono anche dei test strip per il GHB, che pare non siano molto accurati:

<<http://www.wsaw.com/home/headlines/329651.html>>

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

Le News di Counterpane

Intervista a Schneier sul sito Web Netcraft:

<http://news.netcraft.com/archives/2004/08/16/interview_with_bruce_schneier_counterpane_internet_security.html> oppure <<http://tinyurl.com/3s7r7>>

Counterpane ha avuto un secondo trimestre eccellente:

<<http://www.counterpane.com/pr-20040806b.html>>

E il gruppo di analisi Gartner ha riconosciuto ancora una volta la leadership della compagnia nell'ambito del Managed Security Monitoring:

<<http://www.counterpane.com/pr-20040806a.html>>

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

I ranger dell'aeroporto di Houston

Volete contribuire nella lotta contro il terrorismo? Volete essere in grado di fermare e trattenere personaggi sospetti? Oppure semplicemente vi attira l'idea di andare a cavallo lungo dieci miglia di sentieri normalmente chiusi al pubblico? Allora potreste voler partecipare al programma George Bush Intercontinental (IAH) Airport Rangers. Proprio così. Basta compilare un modulo e sottoporvi a un background check, e anche voi potete diventare un combattente di prima linea, poiché l'aeroporto di Houston sta cercando di mantenere la nostra nazione sicura e protetta. L'esperienza non è un requisito fondamentale. Non è nemmeno necessario essere cittadini degli Stati Uniti.

No, non è uno scherzo. Il programma Airport Rangers è volto a promuovere insieme sicurezza e partecipazione da parte della comunità, secondo la descrizione ufficiale. Si tratta di una pattuglia a cavallo costituita da volontari che perlustra i sentieri boscosi incontaminati che formano il perimetro della zona aeroportuale vasta 11.000 acri.

La sicurezza è assai più efficace quando si basa su persone intelligenti e ben addestrate, non certo su individui addestrati per controllare pedissequamente delle fototessere e gli schermi delle macchine a raggi X, e nemmeno sull'implementazione di un profiling che si appoggia a un database. L'idea di guardiani addestrati che perlustrano un perimetro sicuro è buona. Ma in qualità di esperto della sicurezza, vedo un paio di problemi nel programma così come viene presentato.

Il primo problema è la mancanza di addestramento. Il programma incoraggia la partecipazione di "ufficiali autorizzati delle forze dell'ordine", ma non è un requisito fondamentale: chiunque può diventare Ranger. Dalle informazioni che sono riuscito a raccogliere dal sito web, pare che l'addestramento consista in un "breve filmato" su attività sospette. Vi è qualche riferimento ai diritti civili e alle difese costituzionali? Vi è qualche tentativo per evitare il profiling su base razziale? Il profiling è stato un grosso problema persino per gli organi più importanti delle forze

dell'ordine; come se la caverà un gruppo di persone non addestrate? E quali sono le responsabilità dell'aeroporto in caso di problemi?

Il secondo problema è la nuova vulnerabilità di sicurezza che questo programma viene a creare. Il perimetro intorno all'aeroporto è sempre stato terra di nessuno; chiunque venisse visto sulla proprietà risultava immediatamente sospetto. Ora c'è un gruppo di persone autorizzato a percorrere il perimetro dell'aeroporto. Come si riesce a distinguere una persona autorizzata da una che non lo è? Un documento con fototessera, magari osservato da cinque metri di distanza, è facilmente falsificabile. E dato che tutti i Ranger sono a cavallo, se avete un cavallo e un aspetto occidentale, è probabile che sarete considerati automaticamente individui fidati. Grazie a questo programma l'aeroporto è più sicuro o si trova maggiormente a rischio? La risposta è tutt'altro che ovvia.

Al di là di questi due spunti, anche il modulo di adesione rappresenta una lettura interessante. Per partecipare al programma, dovete rinunciare ad ogni genere di diritto. Rinunciate al diritto di contestare il rifiuto arbitrario di una di queste autorizzazioni. Il che potrebbe essere una sorta di compensazione di un altro evidente rischio di questo schema: i background check sono sufficientemente validi per escludere potenziali terroristi? L'intenzione dell'agenzia è per caso quella di effettuare un profiling per proprio conto ed escludere, ad esempio, i musulmani? Una spiegazione più comprensiva potrebbe essere che vorrebbero potersi basare sui rapporti di intelligence senza doverli rendere noti.

La parte più divertente riguarda la certificazione richiesta. I candidati devono dimostrare di non essere membri di note organizzazioni terroristiche. Ciò è ragionevole, ma aspettarsi che dei terroristi dicano la verità sulle loro affiliazioni è un po' ingenuo. Però perché escludere persone che hanno "cause o controversie legali pendenti contro la Città di Houston o l'organizzazione dell'Aeroporto di Houston"? Questo esclude forse chi sta contestando multe per divieto di sosta?

Infine, i candidati devono certificare di non essere membri di nessun gruppo che "sostenga violenze contro [...] una qualsiasi altra nazione". Un anno e mezzo fa una cosa del genere avrebbe escluso tutti i membri dei partiti Repubblicano e Democratico, e qualsiasi altro partito politico a favore dell'invasione dell'Iraq.

<<http://www.houstonairportsystem.org/rangers>>

Questo articolo è apparso originariamente su The Register:

<http://www.theregister.co.uk/2004/07/25/houston_airport_rangers/>

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

Siti Web, password e consumatori

I criminali seguono il denaro. Oggi come oggi, un quantitativo sempre maggiore di denaro si trova in Internet. Milioni di persone gestiscono online i propri conti bancari, i propri account PayPal, il proprio portafoglio azionario o qualsiasi altro genere di conto. È un bersaglio allettante: se un malfattore riesce ad accedere a uno di questi conti, può sottrarre denaro.

E nella maggior parte dei casi questi conti sono protetti soltanto da password.

Se state leggendo questo scritto, probabilmente sapete già che le password non sono sicure. Nel mio libro "Sicurezza Digitale" (era il 2000), scrissi: "Negli ultimi decenni, la Legge di Moore ha reso possibile attuare attacchi di forza bruta su chiavi entropiche sempre più grandi. Allo stesso tempo, esiste una soglia massima dell'entropia che l'utente medio di computer (o anche l'utente sopra la

media) è disposto a ricordare... Questi due valori si sono incrociati; i cracker di password ora sono in grado di decodificare tutto ciò che ci si aspetta venga memorizzato da un utente”.

Su Internet, la sicurezza delle password è in effetti migliore dello scenario appena descritto, perché gli attacchi a dizionario funzionano meglio offline. Un conto è provare ogni chiave possibile sul proprio computer quando si è in possesso del testo cifrato effettivo; mentre è un processo molto più lento quando lo si deve attuare in remoto tramite Internet. E se il sito Web è un minimo astuto, chiuderà l'accesso all'account se vengono effettuati troppi tentativi errati consecutivi (5? 10?) di inserimento password. Se si chiude l'accesso a un account con sufficiente rapidità, è perfino possibile far funzionare i codici PIN a quattro cifre sui siti Web.

Ecco perché i criminali si sono messi a rubare password.

Il cosiddetto phishing è ormai un attacco molto diffuso, ed è sorprendentemente efficace. Pensate a come funziona. Ricevete un messaggio e-mail dalla vostra banca. Il testo del messaggio è assolutamente plausibile, e contiene un URL che sembra proprio provenire dalla vostra banca. Fate clic su di esso, ed ecco apparire il sito Web della banca. Vengono richiesti il vostro nome utente e la password, e voi li inserite. D'accordo, forse voi o il sottoscritto siamo sufficientemente accorti da non inserirli. Ma il comune cliente di home banking non può nulla contro questo tipo di attacco di ingegneria sociale.

E nel giugno 2004 è comparso un Trojan che catturava password. Sembrava un file contenente un'immagine, ma si trattava in realtà di un eseguibile che andava ad installare un'estensione in Internet Explorer. Quell'estensione monitorava e registrava le connessioni in uscita verso i siti Web di una decina fra le maggiori istituzioni finanziarie e poi inviava i nomi utente e le password a un computer in Russia. Usare SSL non serviva a niente: il Trojan registrava le sequenze di tasti prima che le informazioni venissero criptate.

L'industria della sicurezza informatica offre svariate soluzioni migliori delle password: token sicuri che forniscono password usa-e-getta, lettori biometrici, ecc. Ma inviare dell'hardware a milioni di clienti di home banking è così caro da essere proibitivo, sia per quanto riguarda i costi iniziali, sia per l'assistenza al cliente. In più i clienti sono avversi a questi sistemi. E se siete una banca, l'ultima cosa che vorrete fare è creare noie ai vostri clienti.

Ma il fatto che qualcuno sottragga denaro dal vostro conto è ancora più seccante, e le banche stanno rispondendo a un sempre maggior numero di chiamate da parte di clienti vittime di questi attacchi. Anche se il problema di sicurezza non ha niente a che vedere con la banca, anche se il cliente è colpevole di aver commesso l'errore che ha compromesso la sua sicurezza, le banche devono provvedere a indennizzare i clienti. È una delle lezioni più importanti della sicurezza su Internet: a volte i problemi di sicurezza più gravi sono quelli sui quali non si ha il minimo controllo.

Il problema è serio. In un rapporto su sondaggi effettuati in maggio, Gartner ha calcolato che circa 3 milioni di americani sono stati vittime di attacchi phishing. “Perdite dirette dovute a furti d'identità ai danni di vittime di attacchi phishing (fra cui frodi su conti bancari, carte di credito, libretti di risparmio) sono costati alle banche statunitensi e alle compagnie di carte di credito circa 1,2 miliardi di dollari lo scorso anno” (nel 2003). I Trojan e dispositivi quali keyboard sniffer faranno aumentare queste cifre nel 2004.

Anche se le istituzioni finanziarie rimborsano i clienti, l'inevitabile conseguenza è che le persone inizieranno a perdere fiducia in Internet. L'utente medio di Internet non comprende le problematiche di sicurezza: crede che l'icona a forma di lucchetto dorato nell'angolo in basso a destra del suo browser significhi sicurezza. Se questa sicurezza non sussiste (e tutti sappiamo che non sussiste), allora egli smetterà di usare applicazioni e siti Web finanziari.

Le soluzioni sono tutt'altro che semplici. L'infinita serie di vulnerabilità di Windows limita l'efficacia di una qualsiasi soluzione software che si appoggi sull'utente (certificati digitali, plug-in, e così

via), e la facilità con cui del software malevolo può girare su Windows limita l'efficacia di altre possibili soluzioni. Soluzioni specifiche potrebbero costringere gli aggressori a cambiare tattica, ma non risolveranno le insicurezze sottostanti. La sicurezza informatica è una sorta di corsa agli armamenti, e il denaro genera aggressori sempre più motivati. Se dovesse rimanere irrisolto, questo tipo di problema di sicurezza potrebbe modificare il modo con cui le persone interagiscono con Internet. E darà ragione ai disfattisti che hanno sempre sostenuto come Internet non sia sicura per attuare il commercio elettronico.

Phishing:

<<http://www.msnbc.msn.com/id/5184077/>>

<<http://www.internetweek.com/e-business/showArticle.jhtml?articleID=22100149>> oppure

<<http://tinyurl.com/54b4g>>

Il Trojan:

<http://news.com.com/Pop-up+program+reads+keystrokes%2C+steals+passwords/2100-7349_3-5251981.html> oppure <<http://tinyurl.com/yqeo>>

<<http://www.pcworld.com/news/article/0%2Caid%2C116761%2C00.asp>>

Una versione ridotta di questo articolo è apparsa originariamente su IEEE Security and Privacy:

<<http://csdl.computer.org/comp/mags/sp/2004/04/j4088abs.htm>>

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

Commenti dei lettori

Da: Daniel Staal <DStaal@usa.net>

Oggetto: Il giusto processo e la sicurezza

“Un potere di polizia o militare fuori controllo è una minaccia per la sicurezza -- una minaccia grave quanto il terrorismo incontrollato. Non c'è ragione di sacrificare il primo per ottenere il secondo. Ci sono più che valide ragioni per non farlo.”

Volevo solo prendere spunto da questa sua affermazione, ed ampliarla, poiché ritengo che i controlli sul potere militare e di polizia siano *più importanti* di quelli sul terrorismo.

Il terrorismo esiste perché le persone non credono di essere ascoltate dai governi in carica: è un sistema per fare in modo che la propria voce venga ascoltata (un terribile sistema, ma semplice da utilizzare). Gli Stati Uniti sono stati storicamente quasi del tutto immuni ad attacchi terroristici proprio grazie ai loro controlli sul potere di polizia, militare e politico. Grazie a quei controlli, il terrorismo *non è necessario* negli Stati Uniti: una voce può essere ascoltata anche senza di esso (solitamente).

La perdita di quei controlli e l'erosione dei diritti non faranno altro che incoraggiare il terrorismo, perché diverrà chiaro che vi sono pochi modi (e sempre più difficili) per far sì che una voce fuori dal coro sia ascoltata. In tali circostanze, un attacco terroristico è un modo emotivamente soddisfacente per far sentire la propria voce.

Se non si può più contare sul fatto che il governo ascolti le persone, lo si dovrà obbligare a farlo. Il governo degli Stati Uniti ha un'influenza su una popolazione superiore a quella dei propri cittadini, per cui deve rispettare la voce di molte più persone (rispettare non significa necessariamente adeguarsi, ma ascoltare, comprendere e tenere in considerazione). Così facendo il paese sarà più sicuro. Agendo diversamente si renderà il paese meno sicuro.

L'America ha dimostrato che la libertà *è* sicurezza, attraverso la propria storia (fate un confronto con qualsiasi altra nazione paragonabile per status nella storia, controllando il numero di attacchi

terroristici, insurrezionali, rivoltosi: l'America ne ha meno di tutti). È triste vedere come in sempre più parti del paese ormai si cominci a pensare di essere gli uni contro gli altri.

Il potere militare e di polizia non controllato è una minaccia per la sicurezza personale, e aumenta il rischio di attacchi terroristici. Il terrorismo non controllato aumenta il rischio di attacchi terroristici e nient'altro. Statisticamente, se entrambi sono possibili, dal primo ricavo un rischio maggiore, e potenzialmente ho molto più da perdere.

Da: Jeff Evarts <riventree@earthlink.net>

Oggetto: La sicurezza e i dispositivi di archiviazione portatili

Quando osservo i telefoni cellulari, gli iPod, e tutta la schiera di oggetti semi-intelligenti, collegabili e con capacità di archiviazione, non li vedo come veicoli di furti intenzionali di dati, ma come mezzi utilizzabili da hacker malevoli per penetrare all'interno di organizzazioni. Il cellulare Bluetooth di un impiegato viene compromesso (in remoto), l'ignara vittima si reca al lavoro, il cellulare manomesso si impadronisce di tutta una serie di dati accessibili via Bluetooth, che poi vengono scaricati (in remoto) senza che per un momento l'impiegato sia al corrente di quel che accade. Il dispositivo proibito è visto come un vettore di potenziali problemi, non come uno strumento diretto per compiere atti illeciti. Essenzialmente, il divieto assomiglia a quei sensori di calore usati in quelle parti dell'Asia vulnerabili alla SARS per tenere lontano gli impiegati febbricitanti dal posto di lavoro. Quel che preoccupa quei tizi, a mio avviso, è il problema "in seconda", non l'impiegato che sottrae dati e informazioni intenzionalmente.

Da: Eric Vanhove <eric_vanhove@hotmail.com>

Oggetto: Le macchine a raggi X e la sicurezza negli edifici

I suoi commenti alla sicurezza "inadeguata" dell'azienda "FinCorp" sono stati interessanti, ma non hanno tenuto conto di una delle sue proprie affermazioni chiave: quella secondo cui è necessario comprendere il contesto che sta dietro una decisione. Anzitutto, uno dei principi fondamentali della sicurezza è quello di far credere all'aggressore (terrorista, criminale, ecc.) che voi siate un bersaglio molto più difficile di altri. Se riuscite nell'intento (convincere l'aggressore a rivolgersi altrove) semplicemente installando un metal detector, assumendo qualcuno al minimo salariale per controllare un monitor, e facendo perlustrare il perimetro dell'edificio da un cane anti-bomba qualche giorno alla settimana, allora il vostro primo livello di sicurezza è stato raggiunto con successo. Ecco perché la compagnia di assicurazioni ha tutta l'intenzione di offrire lo sconto alla FinCorp. Non è molto diverso da quel che fanno le compagnie di assicurazioni auto con la sicurezza dei veicoli; si ottiene uno sconto anche installando il più banale degli allarmi che (a) verrà ignorato dalla maggior parte delle persone quando si innescherà, e (b) non darà la benché minima preoccupazione al ladro di auto professionista. In secondo luogo, in ogni decisione c'è sempre un minimo di assunzione di rischio. Un sistema di sicurezza più efficace potrebbe comprendere cinque o sei barriere di ingresso attraverso le quali condurre vari tipi di controllo, magari anche una perquisizione completa con svestizione. Ma questo (per svariate ragioni) potrebbe essere estremamente costoso, e una di quelle ragioni potrebbe essere che nessuno, visto quel sistema, voglia più fare affari con la FinCorp. Nessuna decisione viene presa nel vuoto, e la FinCorp ha preso una decisione di business che presume un livello di rischio.

Lei ha trovato alcune pecche nel loro sistema. Se lei fosse un malfattore, metterebbe la FinCorp sulla sua lista di bersagli in una posizione più alta rispetto ad un'altra azienda senza metal detector e cani da guardia. Ma nella scelta di un bersaglio, lei potrebbe usare questo come fattore discriminante per poi decidere di colpire qualcun altro.

Da: Owen Yamauchi <owen.yamauchi@chello.be>

Oggetto: ICS Atlanta

Vi sono moltissime caratteristiche del sito Web di ICS che farebbero scappare chiunque a gambe levate. Ecco un elenco delle più spaventose da me trovate:

- "Considerata La Natura del programma, reverse engineering, non abbiamo a disposizione per il download nessuna versione demo o trial del prodotto. Facendo questo, Vi aiutiamo a mantenere il vostro codice ancor più al sicuro". Questo mi rende estremamente tranquillo nell'usare Tree! Dopotutto, dato che questi individui sono tutti dei super-esperti di sicurezza, è virtualmente impossibile che il codice di Tree venga illecitamente diffuso, no?

- "Pur non Essendo Avvocati, da Quel Che Comprendiamo Della Legge..." Questa gente irradia fiducia e professionalità, nevvvero?

- "Tree Codifica Gli Stessi Dati In Maniera Differente Ogni Volta Che Vengono Codificati". Non staranno mica semplicemente crittografando sotto una chiave casuale per poi incorporare la chiave nel testo cifrato, neh? Perché questo sì che sarebbe stupido!

- "Tree è un programma di crittazione/decrittazione di file progettato per sventare tutti gli attuali metodi di 'snooping' di dati sensibili proprio grazie al sistema stesso con cui Tree codifica i dati". Sicuro. Lo fanno con un algoritmo segreto, e la maggior parte dei metodi attuali di crittoanalisi di un testo cifrato comprendono la conoscenza dell'algoritmo. Non è nemmeno possibile usare la forza bruta, dato che Tree non possiede una chiave da craccare con la forza bruta! Wow!

- "Le Agenzie Governative Sono Già In Possesso Di Questo Programma? Per ora (maggio 2004) la risposta è no". Pensavate che le agenzie governative avrebbero riconosciuto all'istante il valore della crittografia più sicura al mondo, eh? Che sciocchi sono stati.

- "Il nostro metodo si basa su tecniche e metodi usati da persone come i 'code talkers' della Seconda Guerra Mondiale, o sulla costruzione del linguaggio impiegata dagli Egizi". Si tratta probabilmente di un libro di codici. Ma forse lo tengono custodito sul loro network in un file criptato da Tree, per cui sono sicuro che nessun hacker da strapazzo sarà in grado di impossessarsene.

Scherzi a parte, se stanno cercando di truffare la gente, che si mettano un po' più di impegno nel realizzare il loro sito. Perché quasi ogni parola nella seconda parte è scritta con l'iniziale maiuscola? Vi sono errori grammaticali e ortografici. Le schermate sono di pessima qualità. Da quel che si evince dalle schermate, il programma presenta lo stesso tipo di errori linguistici e lo stesso bizzarro uso del maiuscolo del sito Web.

Se questa non è una burla, allora burle di questo genere non esistono!

Da: "Ken Lavender" <ICS_Atlanta@Charter.Net>

Oggetto: ICS Atlanta

[Nella traduzione si è cercato di mantenere lo stesso stile sgrammaticato dell'originale, compresi gli errori ortografici. N.d.T.]

Sono SCONCENTRATO dai suoi "commenti" fatti sul nostro sito:

< <http://www.schneier.com/crypto-gram-0407.html#9> >

Lei dice delle affermazioni che non sono niente altro che calunnie & diffamazioni. Saranno trattate di conseguenza.

Bugia n.1: "E come dimostrano la sicurezza di Tree? "Più di 100 professionisti in matematica e in computer science al Massachusetts Institute of Technology e al Georgia Tech hanno ricevuto degli

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.

Inoltrate liberamente CRYPTO-GRAM a colleghi ed amici che possano trovare questa pubblicazione di un certo interesse. Viene concessa l'autorizzazione a ristampare CRYPTO-GRAM, a condizione che sia stampata integralmente.

CRYPTO-GRAM è realizzata da Bruce Schneier. Schneier è l'autore dei best seller "Beyond Fear", "Secrets and Lies" [tradotto in Italia col titolo "Sicurezza Digitale"] e "Applied Cryptography", e inventore degli algoritmi Blowfish, Twofish e Yarrow. È il fondatore e CTO di Counterpane Internet Security, Inc., e membro del comitato consultivo dell'Electronic Privacy Information Center (EPIC). Scrive spesso e tiene conferenze in merito alla sicurezza informatica e alla crittografia. Il suo sito Web è all'indirizzo < <http://www.schneier.com> >.

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.