

CRYPTO-GRAM
15 febbraio 2005

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>>

Gli stessi articoli della newsletter sono disponibili sul blog di Bruce Schneier:
<<http://www.schneier.com/blog>>.

** **

In questo numero:

Il programma Secure Flight di TSA
Hacking ai danni di T-Mobile
Le ristampe di Crypto- Gram
Falla in RC4 di Microsoft
News
Volare con un biglietto aereo altrui
Una banca denunciata per una transazione non autorizzata
Le News di Counterpane
La maledizione della "Domanda Segreta"
Autenticazione e relativa scadenza
Commenti dei lettori

** **

Il programma Secure Flight di TSA

Come scrivevo il mese scorso, faccio parte di un gruppo di lavoro per studiare la sicurezza e la privacy di Secure Flight, il programma del Governo americano per mettere a confronto i passeggeri delle linee aeree con una watch list di terroristi. Alla fine ho firmato lo NDA (Non-Disclosure Agreement) che mi permette di avere accesso ai documenti SSI (Sensitive Security Information), ma sono riuscito ad evitare di compilare i moduli per quanto riguarda l'autorizzazione speciale sui documenti SECRET.

Il mese scorso il gruppo si è riunito per la seconda volta.

A questo punto ho quattro conclusioni di ordine generale.

1) Assumendo che occorra implementare un programma per mettere a confronto i passeggeri delle linee aeree con i nomi di watch list antiterrorismo, Secure Flight è un grande passo avanti -- sotto quasi ogni aspetto -- se comparato a quel che è attualmente in vigore. Con questo mi riferisco unicamente al programma di confronto, non ai potenziali utilizzi di dati commerciali o provenienti da terze parti.

2) Il sistema di sicurezza che circonda Secure Flight è pieno di buchi di sicurezza. Vi sono problemi di sicurezza legati a documenti d'identità fasulli, alla verifica dei documenti stessi, alla possibilità di volare utilizzando un biglietto aereo altrui, alle procedure delle linee aeree, ecc. Un terrorista ha a disposizione tantissimi modi per aggirare il sistema che non si può considerarlo un sistema sicuro.

3) Il desiderio di applicare questo sistema ad altri ambiti sarà irresistibile. È davvero facile dire: "Visto che avete questo sistema per beccare i terroristi, perché non usarlo con questo elenco di spacciatori di droga... e, già che ci siamo, ci sarebbe anche da pensare all'evento Super Bowl". Una volta che Secure Flight sarà realizzato, basterà preparare una nuova legge, e avremo un sistema di checkpoint di sicurezza a scala nazionale.

4) Un programma per mettere a confronto i passeggeri delle linee aeree con watch list antiterrorismo non ci rende apprezzabilmente più sicuri, ed è un pessimo modo di spendere i nostri soldi in ambito di sicurezza.

Purtroppo il Congresso ha ordinato che Secure Flight venga implementato, perciò è assai improbabile che il programma sia cancellato. Analizzare l'efficacia del programma in generale, il potenziale mission creep [il processo attraverso il quale i metodi e gli obiettivi di una missione cambiano nel tempo, ndt], e se l'idea generale può essere valida o meno, esula dall'ambito del gruppo di lavoro. In altre parole, la mia prima conclusione è fondamentalmente la sola cosa che interessa loro sentire.

Ma questo vuol anche dire che posso scrivere di tutto il resto.

Per tornare alla mia quarta conclusione: immaginate per un momento che Secure Flight sia perfetto. Ovvero, che possiamo essere sicuri che nessuno sia in grado di volare sotto falso nome, che le watch list contengano informazioni perfette sulle identità, e che Secure Flight possa determinare precisamente se un passeggero si trova su una watch list: nessun falso positivo e nessun falso negativo. Anche se arrivassimo a un risultato tale, Secure Flight non varrebbe lo sforzo.

Secure Flight è un sistema passivo. Aspetta che i "cattivi" comprino un biglietto aereo e cerchino di imbarcarsi. Se i "cattivi" non prendono aerei, il tutto diventa uno spreco di denaro. Se i "cattivi" cercano di far esplodere centri commerciali invece che aerei, tutto questo è ancora una volta uno spreco di denaro.

Se io avessi milioni di dollari da spendere in sicurezza antiterrorismo, e se avessi una watch list di potenziali terroristi, investirei i miei soldi facendo indagini su quelle persone. Cercherei di determinare se essi siano stati o meno una minaccia terroristica prima che arrivassero all'aeroporto, o anche nel caso non avessero avuto alcuna intenzione di recarsi ad un aeroporto. Tenterei di prevenire il loro piano a prescindere dal fatto che possano esserci degli aerei di mezzo. Lascerei in pace gli innocenti e perseguirei i colpevoli. Non realizzerei una infrastruttura computerizzata di tale complessità e poi aspettare che un terrorista si aggiri in un aeroporto. Non ha alcun senso, da un punto di vista di sicurezza.

La mia solita metrica quando penso a una misura di sicurezza antiterrorismo è: sarà più efficace del prendere quegli stessi soldi per finanziare l'intelligence, l'investigazione, o la risposta alle emergenze (ovvero cose che ci proteggono a prescindere dalla prossima mossa che stanno progettando i terroristi)? Il denaro speso in misure di sicurezza che funzionano soltanto contro una specifica tattica terroristica, dimenticando quanto i terroristi siano estremamente adattabili, è sommamente sprecato.

Il mio articolo precedente sull'argomento:

< http://www.schneier.com/blog/archives/2005/01/secure_flight_p.html >

** **

Hacking ai danni di T-Mobile

Per almeno sette mesi dello scorso anno, un hacker ha avuto accesso alla rete clienti di T-Mobile. Si è saputo che egli ha avuto accesso a informazioni di 400 clienti (nomi, numeri di previdenza sociale, messaggi in segreteria telefonica, messaggi SMS, fotografie) e probabilmente ha avuto la possibilità di accedere ai dati appartenenti a chiunque dei 16,3 milioni di utenti americani di T-Mobile. Ma nella foga di informare sulla sicurezza dei telefoni cellulari, e di T-Mobile in particolare, i media hanno dimenticato il punto più importante di tutta la vicenda: la sicurezza di molti dei nostri dati non è sotto il nostro diretto controllo.

Questo è qualcosa di nuovo. Una decina d'anni fa o più, se qualcuno voleva spiare la vostra posta, avrebbe dovuto penetrare in casa vostra. Oggi basta che penetri nel vostro ISP. Dieci anni fa, i messaggi vocali erano registrati su una segreteria telefonica in casa vostra; oggi si trovano sul computer di una compagnia telefonica. I vostri dati finanziari si trovano su siti Web protetti solo da password. L'elenco dei libri che cercate e dei libri che acquistate è registrato nei computer di qualche compagnia che vende libri online. La carta di fidelizzazione permette al vostro supermercato di sapere che cibi preferite. Insomma, i dati che una volta erano solitamente sotto il vostro controllo diretto, ora sono controllati da terzi.

Non abbiamo altra scelta se non quella di affidare la nostra privacy a queste aziende, anche se tali aziende non hanno molti incentivi a proteggere quella privacy. T-Mobile ha avuto una pessima pubblicità a causa della sua altrettanto pessima sicurezza, ma niente più. Forse spenderà un po' di soldi per migliorare quella sicurezza, ma si tratterà di sicurezza pensata per proteggere la sua reputazione in sede di pubbliche relazioni, non certo di sicurezza pensata per proteggere la privacy dei propri clienti.

Questa progressiva perdita di controllo sui nostri dati ha anche altri effetti. Le nostre difese contro gli abusi di potere da parte della polizia sono state seriamente diminuite. La corte ha stabilito che le forze dell'ordine possono cercare fra i vostri dati senza alcun mandato, nel caso questi dati siano affidati a terzi. Alla polizia occorre un mandato per leggere i messaggi e-mail sul vostro computer, ma non ha bisogno di un mandato per leggere la vostra posta sui nastri di backup del vostro ISP. Secondo la Corte Suprema, non si tratta infatti di indagine come viene definita dal Quarto Emendamento.

Questo non è un problema tecnologico, ma legale. La corte deve riconoscere che nell'era dell'informazione, la privacy virtuale e quella fisica non hanno gli stessi confini. Noi dovremmo poter avere il controllo dei nostri dati, non importa dove vengano custoditi. Noi dovremmo poter prendere delle decisioni sulla sicurezza e sulla privacy di quei dati e pretendere un ricorso in sede legale se le aziende a cui li affidiamo non rispettano le nostre decisioni. Dato che la Corte Suprema ha finalmente stabilito che tenere sotto controllo un telefono è un'indagine come definita dal Quarto Emendamento, quindi da non poter essere fatta senza un regolare mandato (anche se avesse luogo alla centrale della compagnia telefonica), la Corte Suprema deve riconoscere che leggere i messaggi e-mail altrui presso un ISP è esattamente la stessa cosa.

Questo articolo apparirà su eWeek.

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

Le ristampe di Crypto-Gram

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

Una delle regole più importanti degli stream cipher è quella di non usare mai la stessa keystream per criptare due diversi documenti. Se qualcuno lo fa, è possibile rompere la criptatura effettuando uno XOR sui due stream di testo cifrato insieme. La keystream salta fuori, e si ottiene testo in chiaro XORato con testo in chiaro -- e a quel punto è molto semplice risalire ai due testi in chiaro originari servendosi di tecniche di base quali l'analisi della frequenza delle lettere.

È un errore crittografico da dilettanti. La maniera più semplice per prevenire questo attacco è quella di usare un unico vettore di inizializzazione (IV) in aggiunta alla chiave ogni volta che si cripta un documento.

Microsoft utilizza lo stream cipher RC4 sia in Word che in Excel e incorre in questo errore. Secondo uno studio di Hongjun Wu: "In questo rapporto, evidenziamo una seria falla di sicurezza in Microsoft Word ed Excel. In entrambi i programmi viene usato lo stream cipher RC4 [9] con una chiave lunga fino a 128 bit per proteggere i documenti. Ma quando un documento criptato viene modificato e salvato, il vettore di inizializzazione rimane il medesimo, e in questo modo la stessa keystream generata dallo RC4 viene applicata per criptare le versioni differenti dello stesso documento. Le conseguenze sono disastrose, poiché molte delle informazioni contenute nel documento potrebbero venire facilmente ricuperate".

Tutto ciò non è niente di nuovo. Microsoft ha commesso lo stesso errore nel 1999 con lo RC4 all'interno della Syskey di WinNT. Cinque anni dopo, Microsoft presenta la stessa falla in altri prodotti.

Il rapporto (in formato PDF):

< <http://eprint.iacr.org/2005/007.pdf> >

L'errore commesso da Microsoft nel 1999:

< http://www.bindview.com/Support/RAZOR/Advisories/1999/adv_WinNT_syskey.cfm >

oppure < <http://makeashorterlink.com/?X2862657A> >

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

News

Questo articolo su SIGNAL presenta alcune mie citazioni interessanti:

< <http://www.afcea.org/signal/articles/anmviewer.asp?a=614&z=39> >

Il Dipartimento per la Sicurezza Nazionale sta vagliando un eventuale documento identificativo biometrico per chi lavora nei trasporti. Ho scritto profusamente riguardo agli usi e abusi della biometrica (cfr. "Beyond Fear", pag. 197- 200). In sintesi, la biometrica è ottima come strumento di autenticazione locale e pessima come strumento di identificazione. Per tutta una serie di ragioni, questo progetto del Dipartimento per la Sicurezza Nazionale fa un buon uso della biometrica.

< <http://www.dhs.gov/dhspublic/display?content=4119> >

Una storia terrificante riguardo alla raccolta dati di American Airlines:

< http://www.boingboing.net/2005/01/19/why_is_american_airl.html >

La CIA ha pubblicato un nuovo rapporto che cerca di individuare problematiche globali emergenti che possano richiedere l'azione dei policy maker statunitensi. Val la pena notare che vi sono molti riferimenti alla parola "privacy".

< http://cia.gov/nic/NIC_2020_project.html >

Ufficiali di volo antiterrorismo bloccati da alcuni centimetri di neve:

< <http://www.washingtontimes.com/functions/print.php?StoryID=20050121-122815-8690r>> oppure
< <http://makeashorterlink.com/?F2961157A>>

L'FBI ritira Carnivore:

< <http://www.securityfocus.com/news/10307>>

Naturalmente, non stanno abbandonando la sorveglianza in Internet. Hanno semplicemente capito che gli strumenti commerciali sono migliori, più economici, o entrambe le cose.

Quando telefoniamo a un call center di assistenza clienti, ci imbattiamo tutti nella registrazione che afferma che la chiamata potrebbe essere monitorata. Quel che non realizziamo è che potremmo essere monitorati anche mentre stiamo in attesa. Il controllo ha lo scopo di registrare il comportamento e l'efficienza degli operatori del call center, ma gli spioni professionisti stanno anche involontariamente controllando i chiamanti. La maggior parte di chi chiama non si rende conto che potrebbe venir registrata anche quando resta in attesa. Esiste una semplice difesa per chi è in ufficio e possiede telefoni dotati di tutte le funzioni: il tasto "mute". Ma le persone credono che le loro chiamate siano monitorate "per testare la qualità del servizio o a scopi legati all'addestramento" e danno per scontato che ad essere registrata è soltanto la parte in cui parlano effettivamente con un operatore. Purtroppo anche le difese più semplici non funzionano se le persone non sanno di doverle implementare.

< <http://www.nytimes.com/2005/01/11/business/11snoop.html?ex=1263099600&en=567d8bda6d8b4605&ei=5090>> oppure < <http://makeashorterlink.com/?V2A61157A>>

Uno studio dell'organizzazione di ricerca RAND ha concluso che dotare gli aerei di missili di difesa non è un buon compromesso di sicurezza:

< <http://abcnews.go.com/Technology/wireStory?id=441460>>

Lo RFID come DNA delle automobili:

< <http://www.rfid2vin.com/>>

Un bell'articolo sui conteggi di verifica delle elezioni:

< <http://www.eff.org/deeplinks/archives/002222.php>>

Scoperti, con un hack, tutti i cheat code della PS2:

< <http://www.aquick.org/blog/2005/01/18/all-cheat-codes-for-all-ps2-games-found/>>

oppure < <http://makeashorterlink.com/?R2D62157A>>

"I capi della sicurezza per le elezioni in Iraq allestiranno dei seggi elettorali-esca nel tentativo di ingannare i rivoltosi che hanno promesso di prendere di mira i votanti domenica con uomini-bomba e colpi di mortaio".

< <http://news.scotsman.com/latest.cfm?id=4051297>>

Questo è talmente ridicolo che faccio fatica a credere sia vero. Tutti devono votare, giusto? Ciò significa una cosa fra le due: uno, tutti sanno che i seggi sono esche, per cui i rivoltosi sanno che dovranno evitarli. O due, nessuno sa che sono esche, i votanti ci si radunano comunque, e a quel punto ai rivoltosi non importa che i seggi elettorali siano esche o meno.

Una bellissima foto che illustra bene il principio dell' "anello più debole della catena":

< <http://www.syslog.com/~jwilson/pics-i-like/kurios119.jpg>>

Voci di corridoio non confermate parlerebbero di un virus che infetta le automobili Lexus via Bluetooth.

< <http://www.engadget.com/entry/1234000760029037/>>

La conferenza GovCon esplora tecnologie di intelligence e di prevenzione del terrorismo. C'è una traccia su "le tecnologie necessarie per ottenere una sorveglianza continuativa e per adattarne al meglio la persistenza".

< <http://www.ncsi.com/govcon05/index.shtml>>

Nel tentativo di proteggerci dal terrorismo, vi sono nuove restrizioni sulla vendita di fertilizzanti in Kansas (e altrove):

< <http://www.kansasconnection.com/story-state.cfm?id=36&yr=2005> >

Una compagnia ha messo in commercio un liquido con un identificatore unico. L'idea sarebbe questa: io passo questo liquido sui miei oggetti di valore come prova di proprietà. Io credo che un'idea migliore sarebbe quella di passare il liquido sui vostri oggetti di valore e poi denunciarvi alla polizia.

< <http://www.smartwater.com/products/securitySolutions.html> >

** **

Volare con un biglietto aereo altrui

Recentemente, Slate ha pubblicato un sistema che permette a chiunque di volare con un biglietto aereo altrui.

Ho scritto di questa precisa vulnerabilità un anno e mezzo fa. La vulnerabilità è ovvia, ma i concetti generali sono più sottili. Vi sono tre cose da verificare: l'identità del viaggiatore, la carta d'imbarco, e la registrazione a computer. Pensiamo a queste tre cose come ai tre vertici di un triangolo. Con il sistema attuale, la carta d'imbarco viene confrontata con il documento di identità del viaggiatore, e poi la carta d'imbarco viene confrontata con la registrazione a computer. Ma dato che il documento d'identità non viene mai confrontato con la registrazione a computer (il terzo lato del triangolo), è possibile creare due diverse carte d'imbarco senza che nessuno se ne accorga. Ecco perché l'attacco funziona.

L'articolo di Slate:

< <http://slate.msn.com/id/2113157/fr/rss/> >

Il mio articolo apparso in precedenza:

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

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

** **

Una banca denunciata per una transazione non autorizzata

Un correntista sta denunciando la sua banca perché la somma pari a 90.000 dollari è stata trasferita dal suo conto online da qualcuno che si è impadronito della sua password.

La tipica copertura dei media su questa faccenda è nei termini di "Denunciata la Bank of America perché il PC di un cliente è stato vittima di un hack", ma non è esattamente così. La Bank of America è stata denunciata perché ha permesso che una transazione non autorizzata avesse luogo, e non sta agendo come promesso in merito a quell'errore. La transazione ha potuto aver luogo perché il PC del cliente è stato vittima di un hack.

Non conosco i dettagli della causa legale, ma ritengo che questo sia un problema che non sparirà. Se da un lato penso che le banche non debbano essere ritenute responsabili per quel che risiede sui computer dei loro clienti, dall'altro esse dovrebbero essere ritenute responsabili per aver permesso transazioni non autorizzate. I sistemi interni alla banca, per una ragione o per l'altra, non importa quanto bene siano stati regolati, hanno permesso che avvenisse la transazione fraudolenta.

Il problema qui è di semplice incentivo economico. Finché le banche non risponderanno delle perdite di denaro derivate da transazioni fraudolente via Internet, le banche non avranno alcun incentivo per

migliorare la sicurezza. Ma se venissero ritenute responsabili per queste transazioni, allora potete scommettere che una sicurezza così scadente non sarà più permessa.

< <http://www.sun-sentinel.com/news/local/southflorida/sfl-zlopez05feb05.0.7861225.story> > oppure
< <http://makeashorterlink.com/?X2E61257A> >

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

Le News di Counterpane

Counterpane ha annunciato l'uscita di Enterprise Protection Suite 2.0, un completo servizio di sicurezza che comprende il nostro Managed Security Monitoring, carrier level protection, e l'e-mail scanning.

< <http://www.counterpane.com/pr-20050215a.html> >

Counterpane ha annunciato risultati davvero ottimi per il 2004:

< <http://www.counterpane.com/pr-20050201.html> >

Gartner ha commentato a riguardo dell'alleanza fra Counterpane e Getronics, senza dimenticare l'apertura del nuovo centro operativo Counterpane/Getronics Europeo:

< http://www3.gartner.com/DisplayDocument?doc_cd=126055 >

Schneier interverrà alla RSA Conference a San Francisco. Sarà in una tavola rotonda sulle regolamentazioni (il 16 febbraio alle 8:00) e terrà un discorso sul pensare la sicurezza (il 15 febbraio alle 17:30).

Schneier interverrà al meeting AAAS a Washington DC il 21 febbraio. La tavola rotonda è intitolata "Privacy and Security: Making Intelligent Tradeoffs" [Privacy e Sicurezza: trovare compromessi intelligenti].

Counterpane è alla ricerca di un System Engineer EMEA:

< <http://www.counterpane.com/jobs.html> >

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

La maledizione della "Domanda Segreta"

È capitato a tutti noi: ci registriamo per un qualche account online, scegliamo una password difficile da ricordare e da indovinare, e poi ci viene richiesta una "domanda segreta" a cui rispondere. Vent'anni fa c'era una sola domanda segreta: "Qual è il nome da nubile di vostra madre?". Oggi ce ne sono di più: "Qual è il nome della strada in cui siete cresciuti?", "Come si chiamava il vostro primo animale domestico?", "Qual è il vostro colore preferito?", e così via.

Lo scopo di tutte queste domande è il medesimo: fungere da "password di scorta". Se vi dimenticate la password, la domanda segreta può verificare la vostra identità, poi potete scegliere un'altra password principale o richiedere che la vostra password originaria vi sia spedita via e-mail. È un'ottima idea se vista nella prospettiva del cliente -- è più difficile che un utente dimentichi il nome del suo primo animale domestico che non una password qualsiasi -- ma è una pessima idea vista in un'ottica di sicurezza. È più semplice indovinare la risposta alla domanda segreta rispetto a una buona password, e l'informazione è maggiormente di pubblico dominio (scommetto che il nome del mio primo animale domestico è in giro in qualche database). A peggiorare le cose, pare che tutti usino le stesse serie di domande segrete.

Il risultato è che il normale protocollo di sicurezza (password) fa ricorso a un protocollo molto meno sicuro (le domande segrete) e la sicurezza di tutto il sistema ne soffre.

Che cosa si può fare? La mia solita tecnica è quella di scrivere una risposta completamente casuale -- batto freneticamente sulla tastiera per qualche secondo -- e poi me ne infischio. Questo mi assicura che un aggressore non può aggirare la mia password cercando di indovinare la risposta alla mia domanda segreta; certo, se mi dimentico la password è un problema. L'unica volta che mi è successo ho dovuto chiamare la compagnia per far azzerare sia la password che la domanda segreta (in tutta onestà non ricordo come ho fatto ad autenticarmi con l'operatore del customer care dall'altra parte del telefono...).

Che è forse quello che avrebbe dovuto accadere da subito. Mi piace pensare che se dimentico la password, dovrebbe essere davvero arduo avere accesso al mio account. Voglio che sia così difficile che un aggressore non ci riesca. So che è un problema di customer care, ma è anche un problema di sicurezza. Se la password controlla l'accesso a qualcosa di importante (come il mio conto in banca), allora il sistema per aggirare la password dovrebbe essere più difficile, non più semplice.

Le password hanno raggiunto il termine del loro ciclo vitale di utilità. Oggi vanno bene solo per applicazioni a bassa sicurezza e la "domanda segreta" è solo una delle tante manifestazioni di questo fatto.

Questo articolo è originariamente apparso su ComputerWorld:

< <http://www.computerworld.com/securitytopics/security/story/0,,99628,00.html> >

oppure < <http://makeashorterlink.com/?X2F61457A> >

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

Autenticazione e relativa scadenza

Esiste un problema di sicurezza con molti sistemi di autenticazione su Internet di cui non si parla mai: non c'è modo di terminare l'autenticazione.

Un paio di mesi fa ho comprato qualcosa da un sito di e-commerce. Arrivato alla pagina per il pagamento, non ho potuto semplicemente inserire il mio numero di carta di credito e completare l'acquisto. Ho dovuto invece scegliere un nome utente e una password. Di solito non mi piace farlo, ma in questo caso volevo poter accedere al mio account in un secondo momento. Infatti la password mi è stata utile perché ho poi avuto bisogno di restituire un oggetto da me acquistato.

Sono passati dei mesi, ed è mio desiderio interrompere la relazione fra me e quel sito di e-commerce. Non voglio più un nome utente e una password. Non voglio che essi conservino il mio numero di carta di credito. Ho ricevuto ciò che ho comprato, sono contento, basta così. Invece no, perché visto che quel nome utente e quella password non hanno una "data di scadenza", sono virtualmente eterni. Non è un servizio di iscrizione, per cui non c'è un meccanismo per interrompere le comunicazioni. Avrò accesso a quel sito di e-commerce finché il mio nome utente e la mia password verranno ricordate dal sito stesso.

In altre parole, sono responsabile di quell'account per sempre.

Tradizionalmente, le password sono sempre state indicative di un rapporto continuativo fra un utente e un qualche servizio informatico. A volte si tratta dell'impiegato di un'azienda e i server dell'azienda. Altre volte si tratta di un account e di un ISP. In entrambi i casi, entrambe le parti vogliono che il rapporto continui, per cui far scadere una password e poi obbligare l'utente a sceglierne un'altra è una questione di sicurezza.

In casi con questo rapporto continuativo, la considerazione di sicurezza che viene fatta è la minimizzazione dei danni. Nessuno vuole che un aggressore scopra la password, e tutti vogliono minimizzare i danni che potrebbero subire se egli la scopre. Cambiare periodicamente la password è una soluzione al problema.

Questo approccio funziona perché entrambe le parti lo vogliono; entrambe vogliono che il sistema di autenticazione continui a funzionare correttamente e che si possano ridurre gli attacchi.

Nel caso del sito di e-commerce, gli interessi sono più di una delle due parti. Il sito di e-commerce vuole che io stia nel loro database per sempre. Vogliono farmi delle offerte, e indurmi a ritornare. Vogliono vendere i dati che mi riguardano (questo è il genere di informazioni che potrebbe essere nascosto nei metodi di trattamento della privacy o nei cosiddetti termini del servizio, ma nessuno legge quelle postille perché sono illeggibili. Non è possibile far molto se la compagnia cambia gestione).

Non c'è niente che io possa fare riguardo a tutto ciò, ma un nome utente e una password che non scadono mai è tutta un'altra cosa. Il sito di e-commerce vuole che io crei un account perché questo fa aumentare le possibilità che io mi servirò ancora di loro. Ma io voglio un sistema per porre fine alla relazione commerciale, un modo per dire "d'ora in avanti non mi assumo più alcuna responsabilità per prodotti acquistati usando quel nome utente e password".

Posso dire che il nome utente e la password che ho inserito in quel sito di e-commerce mettono a rischio la mia carta di credito fino alla sua scadenza. Se il sito di e-commerce utilizza un sistema che addebita somme sul mio conto corrente ogni volta che mando un ordine, potrei essere a rischio per sempre. Gli Stati Uniti hanno dei limiti di responsabilità legale, ma non sono molto utili. Secondo la Regulation E, che regola i trasferimenti per via elettronica, una transazione fraudolenta deve essere riferita entro due giorni per restringere la responsabilità nell'ordine di 50 dollari; entro 60 giorni, si arriva a 500 dollari. Oltre quel limite, nulla da fare.

Questo è sbagliato. Ogni sito di e-commerce dovrebbe avere un sistema per permettere l'acquisto di oggetti senza necessariamente dover creare un nome utente e password. Mi piacciono quei siti che mi permettono di comprare qualcosa come "ospite", senza costringermi a creare un account.

Ma, cosa altrettanto importante, ogni sito di e-commerce dovrebbe poter fornire ai clienti un modo per porre termine ai loro account, consentendo loro l'eliminazione dei loro nomi utente e password dal sistema. Sta bene fare offerte commerciali ai vecchi clienti. Non va bene metterli inutilmente a rischio, economicamente parlando.

Questo articolo è apparso anche nel numero di gennaio- febbraio 2005 di IEEE Security & Privacy.

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

Commenti dei lettori

Da: tom <msomefellowjp@yahoo.co.jp>
Oggetto: Prendere le impronte digitali agli studenti

Questa mia vuole essere un feedback per quanto riguarda il concetto di badge identificativo dei bambini che salgono sull'autobus.

Una considerazione molto importante su questo sistema, che non ho visto nel suo pezzo, riguarda la sensibilità e la specificità del test; ovvero, il tasso di falsi positivi e di falsi negativi. Ovvero: quanto è probabile che un badge, registrato come presente sullo scuolabus, significhi che un bambino sia

effettivamente sull'autobus e che non sia stato rapito? Ancora meglio, nel caso in cui il badge non è presente sull'autobus, quanto è probabile che un bambino si sia perso o sia stato rapito?

A chiunque abbia esperienze di lavoro a contatto con bambini sembrerà assolutamente ovvio che un gran numero di bambini non è affatto in grado di custodire badge identificativi e di indossarli come si deve. I badge andranno perduti, saranno ritrovati, verranno scambiati fra i bambini, verranno gettati via, ecc. Due amici si divertiranno a indossare l'uno il badge dell'altro, i ragazzini getteranno i propri e anche quelli di altri bambini a loro antipatici, oppure attaccheranno il badge a qualche zaino che andrà a sua volta perso o dimenticato, eccetera.

È facile prevedere che più di un allarme scatterà ogni giorno, indipendentemente dal fatto che un bambino sia stato rapito o meno, o che si sia perduto o meno. Prevedibilmente, l'imposizione del sistema finirebbe col crescere progressivamente, al punto che ogni giorno l'autista dello scuolabus e il preside della scuola daranno ai bambini minacciosi avvertimenti riguardo all'indossare correttamente il loro badge per tutta la durata del tragitto sull'autobus. I bambini, essendo appunto bambini (e, in questo caso, totalmente a ragione) sentiranno i badge come una misura di sicurezza stupida e umiliante, e non piacerà loro dover indossare quei badge. Tutto questo aggraverà il problema di quei bambini che non porteranno il badge.

In più, la registrazione di un badge che figura come presente sullo scuolabus non significherà necessariamente che anche il bambino sia presente. Un bambino che marina la scuola o che vuole andarsene per conto suo, darà il suo badge a un amichetto. Coppie di fidanzatini condivideranno i loro badge. Gruppi di amici si divertiranno ad attaccare i loro badge sullo zaino di un altro loro amico, e così via.

L'intero sistema proposto è davvero ridicolo e assurdo. Fra tutti i vari test che un sistema di sicurezza proposto dovrebbe passare per essere considerato valido, questo non soddisfa nemmeno uno dei criteri più essenziali: "ci si aspetta che il sistema aiuti effettivamente la gestione del problema in questione".

Da: Jeremy Epstein <jeremy.epstein@cox.net>
Oggetto: Prendere le impronte digitali agli studenti

Oltre ai punti che lei ha già evidenziato, se il sistema di sicurezza viene eluso, allora il tasso di errore potrebbe essere talmente alto da portare costi aggiuntivi per la ricerca dei bambini dispersi. Questo potrebbe far aumentare il costo dell'intero sistema. I bambini, probabilmente, non si sottrarrebbero al sistema deliberatamente, ma qual è il loro incentivo nel venire controllati alla partenza e all'arrivo? L'autista dello scuolabus potrebbe non voler rallentare e perder tempo durante il suo giro in modo che ogni bambino sia registrato, per cui ci potrebbe essere un incentivo a non controllare. [L'articolo citato afferma che fanno uso di RFID, per cui non c'è bisogno che i bambini facciano la scansione, ma potrebbero eluderla tenendo il badge sufficientemente lontano dal lettore... sempre che ce l'abbiano con sé, il badge].

Per quanto riguarda la motivazione (o l'"agenda", come la chiama lei), potrebbe essercene una ancor più semplice: il Dipartimento per la Sicurezza Nazionale sta finanziando ogni sorta di sistema "di aumento di sicurezza", non importa quanto bizzarro. L'articolo che lei cita non offre indicazioni sulla provenienza del denaro, ma potrebbe trattarsi di un "omaggio" al sistema scolastico locale: permette agli ufficiali del luogo di dar l'impressione che stiano facendo qualcosa di concreto, e allo stesso tempo tutto ciò a loro non costa nulla. Per cui, dal loro punto di vista, perché non farlo?

In qualità di genitore di tre bambini che frequentano scuole pubbliche, preferirei che il denaro fosse investito in insegnanti e biblioteche, altro che tracciamento di bambini sugli scuolabus!

Da: Anonimo
Oggetto: Disattivare il network GPS dei cellulari

Nell'ultimo numero di CRYPTO-GRAM, nell'articolo intitolato "Disattivare il network GPS", lei fa riferimento a commenti di varie persone secondo cui dovrebbe esserci un modo di disattivare il network di telefonia mobile (cellulare) in caso di attacco terroristico. Avendo lavorato nell'industria delle telecomunicazioni, so che questa tecnologia esiste ed è stata operativa in diversi paesi per alcuni anni; tuttavia, il pretesto non riguardava attività antiterroristiche, ma l'assistenza dei servizi di soccorso in caso di gravi incidenti.

Se le è mai capitato di trovarsi bloccato in una stazione ferroviaria o all'aeroporto a causa di ritardi, e ha cercato di chiamare qualcuno per avvisarlo dell'inconveniente, avrà notato che a volte è necessario fare diversi tentativi prima di poter collegare la chiamata. Questo avviene perché vi è un numero limitato di celle disponibili alla stazione base per gestire tutte le chiamate all'interno di una data area. In condizioni operative normali, una certa area coprirà diverse migliaia di persone che fanno o ricevono chiamate a intervalli casuali in un certo lasso di tempo. Le stazioni base sono regolate per gestire un numero di chiamate effettuate da una data percentuale delle persone in un dato momento, e nella maggior parte dei casi questo sistema funziona bene. Quando succede qualcosa che coinvolge un gran numero di persone nello stesso momento, ad esempio 300 persone che attendono un treno/aereo in ritardo, la stazione base può raggiungere il massimo di capacità molto rapidamente, e questo impedisce alle persone che stanno chiamando di ottenere una cella. Lei sa questo, lo so io, e lo sanno anche i giornalisti, e qui sta il problema.

Quando accade un evento di una certa importanza, i giornalisti accorrono a frotte sul posto per ottenere storie da inoltrare poi alle rispettive stazioni radiotelevisive. Queste organizzazioni sono in gran competizione fra loro, e ognuna cerca di essere "la prima sul posto" ad avere "lo scoop sensazionale da prima pagina". In pratica questo significa che mandano un giornalista sul posto il prima possibile, e poi il giornalista richiama l'ufficio dal suo telefonino per trasmettere la storia via telefono. I giornalisti sanno come funziona il network di celle e una volta che hanno ottenuto il collegamento con l'ufficio non riattaccano più per paura di perdere la connessione 15 minuti dopo, quando avranno altri particolari da riferire. L'area, e il network di celle, si saturano velocemente e ciò impedisce ai servizi di soccorso di usufruire delle celle.

Per opporsi a questa situazione, c'è un sistema all'interno di certi network di celle che permette di restringere le chiamate, in caso di emergenza, ad alcuni specifici telefoni. Questo elenco di solito contiene i codici IMEI e SIM dei telefoni che sono stati assegnati ai servizi di sicurezza e di emergenza. Se e quando il sistema viene attivato, esso limita immediatamente l'uso del network di celle soltanto a quei telefoni; in moltissime installazioni questo può esser fatto a livello di stazione base, per cui tutti coloro che sono fuori dall'area dell'incidente non ne risentono.

Tale sistema impedisce chiaramente alle altre persone di chiamare casa per dire che stanno bene, ma è stato studiato per attivarsi solo in casi di gravi emergenze e per quegli incidenti in cui la priorità è quella di proteggere e assistere i feriti; poter contattare casa è una bella cosa, ma essere ancora vivi per poter chiamare dopo è ancora più importante.

Da: Mace Moneta <mmoneta@optonline.net>

Oggetto: La sicurezza di Linux contro quella di Microsoft

Credo che lei abbia semplificato un po' troppo la problematica legata a Linux e agli hacker. Credo che nella faccenda siano coinvolte anche etica e filosofia. Gli hacker sono gli anarchici della nuova era, tutti a caccia del grande "uomo". Linux viene creato, mantenuto e distribuito dal "ragazzino", gratuitamente. Si paga solo il supporto tecnico, non il software incluso in una tipica distribuzione Linux. Anche se molte aziende stanno guadagnando milioni di dollari grazie a servizi che si appoggiano su Linux, Linux stesso è eticamente "pulito". L'altro aspetto è che molte attività di hacking vengono condotte per ottenere punti/karma/riconoscimenti all'interno della comunità degli hacker. Dato che Linux è open source, quello stesso riconoscimento pubblico può essere ottenuto grazie ad attività "white hat" -- riferire e individuare vulnerabilità di sicurezza.

In molti hanno detto che quando Linux diventerà grande quanto Windows, verrà anche colpito molto di più. Io non ci credo. Finché Linux rimarrà libero, e lo sviluppo aperto, Linux non rappresenterà un bersaglio. Guardi i recenti commenti di Linus Torvalds (<<http://kerneltrap.org/node/4540>>) sulla gestione delle notifiche di sicurezza. Tenendole di dominio pubblico, quelli che scoprono una falla ottengono un vasto e immediato riconoscimento generale. Questo rappresenterà un vantaggio più grande di quanti oggi nella comunità Linux possono apprezzare. La trasparenza completa permette di rimanere fuori dalla lista dei bersagli degli hacker. Non ci sono "punti" a disposizione per compiti troppo facili...

Da: Jon Tullett <Jon.Tullett@haynet.com>
Oggetto: Il sistema Chip and PIN britannico

Chip and PIN è una buona cosa, in quanto riduce l'evasione fiscale. (Tuttavia, i criminali rimarranno criminali, e se una strada diventa ardua da sfruttare, si faranno venire altre idee. Per cui non servirà a fermare il crimine o i singoli criminali).

Ma, evasione fiscale a parte, quanto c'è di buono? Lascio da parte le transazioni Chip and PIN qui.

Nell'ambito della sicurezza informatica (come lei naturalmente saprà) abbiamo il concetto di sicurezza a due fattori. Di qualcosa che conoscete/avete/siete, prendetene due. Le tessere bancarie già la possiedono: la tessera stessa e un (debole) dato biometrico rappresentato dalla firma. Con il sistema Chip and PIN abbiamo la stessa cosa: la carta e una debole password.

Nell'ambito della sicurezza informatica, tutti sappiamo bene quanto deboli siano le password. La gente se le scrive e le riusa. Nel caso di una persona che possiede molte tessere bancarie e carte di credito, quasi certamente terrà un elenco dei PIN nel portafoglio (per cui, rubato il portafoglio, rubati i PIN), e quasi di sicuro userà lo stesso codice PIN per più tessere (per cui, intercettata una transazione Bancomat, e avrete accesso ad ogni tessera). E, naturalmente, bisogna inserire il PIN _in pubblico_ ogni volta che si usa la tessera.

Per cui abbiamo rinunciato a un debole dato biometrico per avere una password tremendamente debole. Come può essere questa una miglioria?

Inoltre mi chiedo: dato che abbiamo i sistemi e l'esperienza di gestione delle firme con le carte di credito, perché sono state eliminate? Perché non usare Chip and PIN _e_ una firma? Dopotutto ci vuole solo un secondo, e ogni possessore di carte e ogni commerciante hanno ormai familiarità con il sistema della firma.

Un motivo piuttosto ovvio è quello di parare il didietro delle banche e dei commercianti. La firma è utile per i rifiuti, perché le banche devono fornire, su richiesta, lo scontrino firmato per la transazione che io contesto. Se la firma è palesemente falsa, otterrò un risarcimento da parte del commerciante, facilitato dalla banca. Ai commercianti e alle banche questo non piace, per ovvi motivi.

Ma come faccio a provare che non sono stato io a inserire il PIN? Non ho forse io, infatti, appena perso la possibilità di contestare una transazione? Se la mia tessera bancaria viene rubata durante la spesa che faccio settimanalmente, e la dichiaro smarrita solo quando me ne accorgo, cioè durante la spesa che farò la settimana _seguente_, le transazioni svolte durante quell'intervallo di tempo (non dichiarato) non saranno protette.

Per cui, a parte la minor superficialità, pare che abbiamo rinunciato a un dato biometrico per una password, e abbiamo rimosso un meccanismo importante che protegge gli utenti. Un guadagno netto per banche e commercianti, dal punto di vista della loro esposizione e dei loro rischi; ma una perdita netta da parte del consumatore.

C'è forse qualcosa di ovvio che mi sfugge? Tutto questo viene presentato come un punto vincente per i possessori di tessere bancarie, ma non mi sembra che sia proprio così. D'altra parte, so che le

riduzioni dell'evasione fiscale sono state positive in molti paesi, per cui non sono contrario alla cosa in sé. Solo scettico.

Da: Jim Reid <jim@rfc1035.com>

Oggetto: Il sistema Chip and PIN britannico

I suoi commenti riguardanti l'introduzione del sistema chip and PIN da parte delle compagnie britanniche di carte di credito sono un tantino ingiusti. Certo, esiste una campagna pubblicitaria che suggerisce ai possessori di carta di poter usare PIN facili da indovinare. Ad ogni modo, tutto questo serve semplicemente a spiegare al grande pubblico come funziona il sistema chip and PIN e a calmare le paure di chi si trova a disagio ad usare i PIN. Si tratta in gran parte di un esercizio per conquistare cuori e menti. In tale contesto, una spiegazione semplificata della scelta del PIN può aiutare. [Si provino a spiegare le pratiche di corretta gestione delle chiavi in una pubblicità sui giornali o alla TV]. Quando i PIN vengono emessi per le carte nuove, sono accompagnati da un foglio che spiega come si può modificare il codice PIN. Questo in genere comprende una serie di buoni consigli su come scegliere un PIN che può essere facile da ricordare ma non necessariamente facile da indovinare, ad esempio la data di nascita o il numero di telefono di un membro familiare e non il proprio; non usare lo stesso codice PIN del proprio Bancomat; eccetera eccetera.

Fra l'altro, le nuove tessere hanno ancora la striscia magnetica e lo spazio per la firma sul retro. Quando viene usato il PIN, non c'è uno scontrino da firmare e controllare. Non sono sicuro se questa sia una buona cosa o meno.

Da: Matthew Rubenstein <email@mattruby.com>

Oggetto: Terrorismo e Sabotaggio

Terrorismo cibernetico: speravo che lei facesse le sue solite acute distinzioni fra i fattori essenziali del cosiddetto "terrorismo". Far saltare dighe, o centrali nucleari, palazzi di uffici o altre infrastrutture vitali o di grandi dimensioni, in sé, è sabotaggio. Il terrorismo, come qualsiasi altro "ismo", è un credo praticato, non soltanto una pratica. Il sabotaggio senza un'ideologia dietro, come lei dice con termini diversi, è "semplicemente" crimine. Ma la distinzione importante fra sabotaggio e terrorismo, importante nell'ottica di fermarlo, è la pratica stessa. Il terrorismo dipende dal valore di terrore, che può essere trasmesso solo nei media -- compreso il passaparola. Dirottare aerei sul World Trade Center è terrorismo, perché a causa dell'incessante esposizione dei media, il suo messaggio arriverà a destinazione. Non solo perché è un fatto eccezionale, perché ha ucciso un sacco di persone, è stato critico per l'economia di New York City -- ma perché lascerà la traccia per anni grazie alle spaventose immagini mandate per televisione, e la gente non smetterà mai di parlarne.

Occorre una maggiore sofisticazione nei nostri media per sopravvivere integri alla Guerra del Terrore. Ce più bisogno di questo che non addirittura di migliorie a livello di sicurezza. Bin Laden e i suoi simili giocano con i nostri media come vogliono, ci costano miliardi, e dividono e distruggono la nostra società. Il primo scoppio è la miccia necessaria che loro accendono. Ma la bomba è rappresentata dai nostri media ingenui, che si indeboliscono da soli. Ho dato i suoi libri, consigliandone caldamente la lettura, a dirigenti di network di news e a ufficiali del governo cittadino qui a New York e altrove. Mi piacerebbe che lei parlasse di più delle vulnerabilità dei media rispetto al terrorismo, ambito in cui più abbiamo bisogno di riorganizzare il nostro sistema.

Da: "Kimberly Allen" <kimall@mindspring.com>

Oggetto: La Guerra Cibernetica

Nel suo pezzo sulla guerra cibernetica, lei mette in evidenza alcune delle qualità peculiari degli attacchi cibernetici sebbene i loro nomi siano semplicemente identici a quelli di altri attacchi (guerra, terrorismo, crimine, vandalismo) e abbiano in più solo il prefisso cyber- o l'aggettivo "cibernetico". Se da un lato concordo che sia utile pensare in termini di attacchi cibernetici mentre lavoriamo per

comprendere le loro potenziali minacce, contromisure e utilità strategiche, ritengo d'altro canto che tali termini non debbano essere separati all'interno della loro "categoria cibernetica".

La guerra cibernetica è parte della guerra, e non parte di una qualche nuova categoria generale chiamata attacchi cibernetici. Le persone che studiano la guerra conoscono ogni cosa che riguardi la guerra in trincea, le dinamiche di combattimento delle guerriglie all'interno di una giungla, la guerra nel deserto, attacchi aerei per colpire bersagli precisi, ecc., e ora dovranno aggiungere la guerra cibernetica alle loro competenze. Coloro che lavorano sul terrorismo dovranno fare altrettanto con il terrorismo cibernetico; stesso dicasi per crimine cibernetico e vandalismo cibernetico. È solo un altro mezzo da aggiungere al portfolio.

Chiaramente, nelle prime fasi di comprensione di questa problematica, potrebbe essere utile parlare degli attacchi cibernetici come categoria. È estremamente efficace, da parte di persone che provengono da diversi dipartimenti, riunirsi per capire un nuovo metodo di attacco. Ma alla fine essi riporteranno queste conoscenze all'interno dei loro dipartimenti, dove verranno trasformate e specializzate nel genere di informazioni dettagliate di cui hanno davvero bisogno e che possono utilizzare. Prevedo che, col tempo, la comprensione della guerra cibernetica finirà col divergere da quella del terrorismo cibernetico, perché le persone che detengono questa conoscenza torneranno ad incorporarsi nei loro propri dipartimenti. E questo non è completamente sbagliato; il perfezionamento dettagliato delle conoscenze sulla guerra cibernetica non può aver luogo se viene costantemente sincronizzato con la conoscenza sul terrorismo cibernetico.

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

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.

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) 2005 by Bruce Schneier.