

CRYPTO-GRAM
15 maggio 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:

[Blog: Schneier sulla sicurezza](#)

[REAL ID](#)

[È giusto che i media parlino di terrorismo?](#)

[I nuovi rischi connessi agli autovelox](#)

[Le ristampe di Crypto-Gram](#)

[Rilevare materiale nucleare in transito](#)

[Le potenzialità per la realizzazione di un Worm SSH](#)

[News](#)

[Passaporti biometrici nel Regno Unito](#)

[Accendini banditi sugli aeroplani](#)

[Le news di Counterpane](#)

[Campi minati Wi-Fi](#)

[Il Rapporto PITAC sulla Cyber-sicurezza](#)

[Furto d'identità sponsorizzato dallo Stato](#)

[Combattere lo Spam](#)

[Commenti dei lettori](#)

** ** ** ** **

Blog: Schneier sulla sicurezza

Sono ormai otto mesi che pubblico un blog. In esso vi trovate più o meno le stesse cose che potete leggere in Crypto-Gram, solo che gli aggiornamenti sono quotidiani e non hanno cadenza mensile. E cerco poi di revisionare quel che ho pubblicato nel blog quando lo riporto qui. Leggetelo, se vi può interessare.

<<http://www.schneier.com/blog>>

** ** ** ** **

REAL ID

Gli Stati Uniti avranno un documento d'identità nazionale. Il REAL ID Act stabilisce standard uniformati per le patenti di guida dei vari stati, che dovranno entrare in vigore entro tre anni a partire da ora, creando di fatto un documento di identità nazionale. Si tratta di una pessima idea, e ci renderà tutti meno sicuri. Ed è anche molto costosa. E tutto questo è successo senza nemmeno un vero e proprio dibattito in sede congressuale.

Ho già scritto in merito ai documenti d'identità nazionali. Ho già parlato delle convinzioni sbagliate che sussistono intorno all'identificazione come strumento di sicurezza. Non ho intenzione di ripetermi ulteriormente e invito chiunque sia interessato all'argomento di leggere quegli articoli (trovate i link in fondo a questa sezione). Ricordiamoci che la domanda da porsi non è se un documento d'identità nazionale porterà qualche beneficio, semmai la domanda è: quei benefici che porterà saranno sufficienti a giustificarne i costi? In quest'ottica, un documento d'identità nazionale è un pessimo compromesso di sicurezza. E tutti devono capirne il perché.

A parte le questioni di ordine generale contenute nei miei precedenti interventi sul tema, vi sono degli aspetti specifici di REAL ID che concorrono a renderlo un strumento di pessima sicurezza.

Il REAL ID Act richiede che le patenti di guida incorporino "una comune tecnologia leggibile da un dispositivo". Questo, naturalmente, faciliterà i furti di identità. Già alcuni alberghi fanno fotocopie del vostro ID quando vi registrate, e alcuni bar fanno una scansione del vostro ID quando provate a comprare alcolici. Dato che gli Stati Uniti non hanno alcuna legge che protegga i dati sensibili, entità commerciali come alberghi e bar possono rivendere le vostre informazioni a data broker come ChoicePoint e Acxiom. Lo faranno, sarebbe una cattiva mossa commerciale non farlo. In effetti non importa quanto bene i singoli stati e il governo federale proteggano i dati riportati dalle patenti di guida, visto che vi saranno dei database commerciali paralleli con le stesse informazioni.

Quelli che prendono ad esempio le nazioni europee dotate di documenti d'identità nazionali, tengano ben presente questo punto: i paesi dell'Unione Europea possiedono una forte struttura legale di protezione dei dati sensibili e della privacy. Ecco perché l'esperienza americana sarà molto diversa da quella europea, e un danno ben più grave per la società.

Ancor peggio, è molto probabile che in queste nuove patenti di guida verrà incorporato un chip RFID. Le stesse specifiche per l'inclusione di chip RFID nei passaporti comprendono una serie di dettagli per l'inclusione di tali chip nelle patenti. Presumo che il governo federale imporrà ai vari stati di prendere provvedimenti in questo senso, con tutti i problemi di sicurezza associati (per esempio gli accessi non autorizzati).

REAL ID richiede che le patenti di guida riportino indirizzi veri e non indicazioni di eventuali caselle postali. Nessuna eccezione viene fatta per giudici o polizia -- nemmeno per gli agenti che lavorano sotto copertura. Questo pare proprio un inutile e grave rischio di sicurezza.

REAL ID, inoltre, proibisce ai singoli stati di emettere patenti di guida agli immigrati clandestini. Ciò non ha senso, e non farà altro che spingere gli immigrati clandestini a guidare senza patente -- il che non contribuirà alla sicurezza di nessuno. Si tratta di una insicurezza interessante, e rappresenta la conseguenza diretta del prendere un documento -- che è uno specifico permesso di guidare un veicolo -- e di trasformarlo in un mezzo di identificazione generale.

REAL ID è costoso. È un mandato che non viene finanziato dal governo: il governo federale costringe i vari stati a spendere il proprio denaro per uniformarsi alla legge. Ho visto alcune stime secondo le quali la spesa che gli stati dovranno sostenere per conformarsi a REAL ID sarà dell'ordine delle decine di miliardi di dollari. Tutti soldi che non possono essere investiti in vera sicurezza.

Ma la cosa più folle in assoluto è che nulla di questo è necessario. Nell'ottobre 2004 lo Intelligence Reform and Terrorism Prevention Act è stato tramutato in legge. Tale legge includeva misure di sicurezza più forti per le patenti di guida, cioè quelle consigliate dal 9/11 Commission Report. È tutto già stato fatto. È già legge.

REAL ID va ben oltre: è una grande presa di potere da parte del governo federale rispetto ai sistemi di emissione delle patenti di guida dei singoli stati.

Prima che REAL ID entri in vigore devono passare tre anni dal momento in cui diventa legge, ma mi aspetto che le cose saranno di gran lunga peggiorate nel frattempo. Uno dei miei timori è che questa nuova patente di guida standardizzata porti un nuovo livello nei controlli governativi sullo stile "mi mostri i tuoi documenti". Già non è possibile volare senza un documento identificativo, anche se nessuno ha mai spiegato come il controllo di tale documento possa rendere più ardue le azioni terroristiche sugli aerei e negli aeroporti. In precedenza ho scritto di Secure Flight, un altro pessimo sistema di sicurezza che cerca di mettere a confronto le liste dei passeggeri delle linee aeree con non meglio specificate watch list antiterrorismo. Ho già percepito segnali riguardanti l'obbligo, per i vari stati, di controllare le identità servendosi di "database governativi" prima di emettere una patente di guida. Sono certo che il modello di Secure Flight verrà esteso alle navi da crociera, ai treni, e forse addirittura alle metropolitane. Unite REAL ID e Secure Flight e avrete un sistema di sorveglianza su vasta scala della popolazione di un paese, un sistema senza precedenti.

C'è qualcuno che si sentirebbe più sicuro all'interno di un tale stato di polizia?

Gli americani rifiutano in larghissima misura i documenti d'identità nazionale in generale, ed esiste un grandissimo numero di oppositori al REAL ID Act.

Se non avete trovato molte notizie nei giornali in merito a REAL ID, non è un caso. Le manovre politiche intorno a REAL ID hanno quasi del surreale. È stato bocciato ai voti lo scorso autunno, ma è stato reintrodotta e appiccicata alla legislazione che finanzia le azioni militari in Iraq. Si trattava di una parte di legislazione "da passare a tutti i costi", il che vuol dire che non c'è stato alcun dibattito su REAL ID. Nessuna udienza, nessun dibattito nelle commissioni, nessun dibattito in assemblea. Niente di niente. E ora è legge.

Ma non siamo ancora sconfitti. REAL ID può essere osteggiato in altri modi: attraverso finanziamenti, nei tribunali, ecc. Chi fosse seriamente interessato a questa problematica è invitato a partecipare a un evento sul tema, sponsorizzato da EPIC, che si terrà a Washington DC il prossimo 6 giugno. Io ci sarò.

Il testo dello REAL ID Act:

<<http://thomas.loc.gov/cgi-bin/bdquery/z?d109:h.r.00418:>>

L'analisi di Congressional Research Services:

<<http://www.eff.org/Activism/realid/analysis.pdf>>

I miei interventi precedenti sull'identificazione e sui documenti d'identità nazionali:

<<http://www.schneier.com/crypto-gram-0404.html#1>>

<<http://www.cryptogram.it/cryptogramPdf/Aprile2004.pdf>> (traduzione in italiano)

<<http://www.schneier.com/crypto-gram-0402.html#6>>

<<http://www.cryptogram.it/febbraio04.htm>> (traduzione in italiano)

<<http://www.schneier.com/crypto-gram-0112.html#1>>

I problemi di sicurezza con i RFID:

<<http://www.schneier.com/crypto-gram-0410.html#3>>

I miei articoli precedenti su Secure Flight:
<<http://www.schneier.com/crypto-gram-0502.html#1>>

Altre risorse:
<http://www.epic.org/privacy/id_cards/>
<<http://www.unrealid.com/>>

L'evento sponsorizzato da EPIC a Washington DC:
<<http://www.epic.org/events/id/savethedate.html>>

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

È giusto che i media parlino di terrorismo?

In un editoriale d'opinione, il giornalista John Tierney ha sostenuto come i media stiano svolgendo un pubblico disservizio parlando di tutti gli attentati dinamitardi suicidi in Iraq. Tutto questo non fa altro che spaventare la gente, ha affermato, e finisce col fare il gioco dei terroristi.

Alcuni blogger liberali hanno attaccato questo editoriale, accusandolo di incoraggiare i tentativi dell'attuale amministrazione di nascondere gli orrori della guerra in Iraq all'opinione pubblica americana. Credo tuttavia che la questione sia un filo più sottile. Prima di comprendere perché la posizione di Tierney sia sbagliata, è necessario capire che egli ha ragione in merito ad alcuni aspetti del problema.

Il terrorismo è un crimine contro la mente. Il vero obiettivo di un terrorista è il morale, lo stato d'animo, e la copertura della stampa lo aiuta ad ottenere il suo scopo. In "Beyond Fear" ho scritto (pagg. 242-3):

"Lo stato d'animo è il principale obiettivo di un terrorista. Rifiutandoci di farci spaventare, rifiutandoci di reagire in modo eccessivo, e rifiutandoci di pubblicizzare in continuazione gli attacchi terroristici tramite i mass media, possiamo ridurre l'efficacia degli attacchi terroristici stessi. Durante la gran quantità di attentati dinamitardi da parte dell'IRA in Inghilterra e Irlanda del Nord negli anni Settanta e Ottanta, la stampa capi che i terroristi volevano che il governo Britannico reagisse in modo eccessivo, e così decise di trattenersi; una scelta che venne poi encomiata. La stampa statunitense non ha dimostrato un'analogha comprensione dello stato delle cose nei mesi immediatamente successivi alla tragedia dell'11 settembre, e ha dato modo al governo degli Stati Uniti di reagire eccessivamente.

Provate a ragionare in questo modo. Se la stampa non avesse riportato gli attacchi dell'11 settembre, se la maggior parte delle persone negli Stati Uniti non ne avesse saputo nulla, allora quegli attacchi non sarebbero stati un momento così cruciale nella nostra politica nazionale. Se avessimo vissuto 100 anni fa, e la gente avesse letto soltanto le notizie sui giornali e avesse visto solo delle fotografie degli attacchi, allora non ci sarebbe stata una tale reazione emotiva. Se avessimo vissuto 200 anni fa, e le uniche cose a nostra disposizione fossero state i resoconti scritti e orali, la reazione emotiva a un tale evento sarebbe stata ancora minore. Il tipo di copertura della notizia che abbiamo ora amplifica le azioni terroristiche trasmettendole di continuo, con filmati e sonoro, imprimendole nella psiche di ogni spettatore.

Così come l'attenzione dei media per l'11 settembre ha spaventato le persone inducendole ad accettare reazioni esagerate da parte del governo (come il PATRIOT Act), l'attenzione dei media per gli attentati dinamitardi suicidi in Iraq induce la gente a credere che l'Iraq sia più pericoloso di quanto lo è in realtà.

Tierney scrive:

“Non sto sostenendo una censura ufficiale, tuttavia non vedo perché i media non possano attenuare la propria eccessiva indulgenza nel trattare gli attentati dinamitardi. Un minimo di moderazione darebbe al pubblico una prospettiva più realistica dei pericoli nel mondo.

“Così come i cittadini di New York hanno imparato a prestare più attenzione alle statistiche dei reati che non al baccano e ai sensazionalismi delle news della sera, le persone potrebbero finalmente iniziare a credere alle statistiche che dimostrano come le probabilità di essere uccisi da un terrorista, in Iraq o in qualsiasi altra parte del mondo, sono straordinariamente basse”.

Ho sostenuto praticamente la stessa cosa, anche se in maniera più generale, in “Beyond Fear” (pag. 29):

“I moderni mass media, specialmente i film e i telegiornali, hanno degradato la nostra percezione di un pericolo naturale. Veniamo a conoscenza di certi rischi (o riteniamo di conoscerli) non mediante un'esperienza diretta del mondo che ci circonda e osservando quel che capita ad altri, ma, e in sempre maggior misura, ricavando la nostra visione delle cose attraverso la lente distorta dei media. La nostra esperienza viene distillata per noi, e risulta essere un campione che manda a monte le nostre percezioni. I ragazzini provano a imitare delle acrobazie che hanno visto in TV fatte da stuntman professionisti, senza mai tener presenti le precauzioni che questi professionisti mettono in pratica. Le notizie al telegiornale della sera non riflettono veramente il mondo in cui viviamo, ma soltanto alcune piccole, particolari porzioni di esso.

“Vengono ingranditi ed evidenziati quei quadri di vita dotati di un impatto visivo immediato; invece, quelli che non hanno una componente visuale, o che non possono essere assimilati immediatamente e in maniera istintiva, sono privati di ogni enfasi. Rarità e anomalie, come il terrorismo, vengono discusse e dibattute continuamente, mentre rischi comuni come le malattie cardiache, il cancro al polmone, il diabete e il suicidio vengono minimizzate.

“La portata globale delle news di adesso non fa altro che acutizzare il problema. Se un bambino viene rapito a Salt Lake City durante l'estate, ogni madre in ogni stato del paese si preoccupa immediatamente del rischio che possono correre i propri figli. Se vengono riportati degli attacchi da parte di squali sulle coste della Florida -- e magari fanno anche un film sul tema -- improvvisamente ogni nuotatore è preoccupato (ogni anno molte persone vengono uccise più dai maiali che dagli squali, il che mostra quanto bravi siamo a valutare un rischio)”.

Una delle cose che dico più spesso agli altri è: se è nelle news, non preoccupatevi. Per definizione, la parola “news” (lett. “nuove”) implica un qualcosa che succede molto raramente. Se le news parlano di un certo rischio, allora con ogni probabilità non vale la pena preoccuparsene. È quando non si parla più di una cosa (morti provocate da incidenti stradali, violenza domestica, ecc.), quando questa cosa diventa talmente “normale” da non far più notizia, che occorre iniziare a preoccuparsi.

Tierney sostiene la propria posizione con la prospettiva di chi ritiene che l'amministrazione Bush stia facendo un buon lavoro nella lotta antiterrorismo, e che i reportage dei media sugli attentati dinamitardi suicidi in Iraq stiano affievolendo il desiderio di combattere da parte degli americani. Io invece osservo la stessa problematica da un punto di vista opposto, ovvero con la prospettiva di chi ritiene che i reportage dei media sulle minacce e sugli attacchi terroristici abbia aumentato il supporto dell'opinione pubblica a favore delle draconiane leggi antiterrorismo dell'amministrazione Bush e a favore di una politica interna ed estera pericolose e dannose. Se i media non avessero riportato ogni allarme, ogni avviso, ogni arresto condotto dall'amministrazione, ora in America avremmo una politica antiterrorismo molto più sensibile e saremmo tutti molto più al sicuro.

E allora perché quanto dice Tierney è sbagliato? È sbagliato perché il pericolo insito nel non parlare degli attacchi terroristici è più grande del rischio connesso al parlarne in continuazione. La libertà di stampa è una misura di sicurezza. L'unico mezzo che abbiamo per mantenere

la maggior parte degli automobilisti adesso viaggia poco sotto le 79 miglia orarie, che è la soglia oltre la quale si viene multati”.

In risposta agli autovelox, gli automobilisti stanno adottando l'ovvia strategia di guidare appena poco al di sotto del limite di velocità che innesca le telecamere, presumibilmente tenendo una velocità costante. Perciò, invece di esserci sulla strada delle vetture che viaggiano entro uno spettro di velocità con distanze ragionevoli fra di esse, assistiamo a “gruppi” (nel senso ciclistico del termine) di auto che viaggiano tutte insieme alla stessa (alta) velocità, rappresentando un pericolo inusitato per se stesse e per tutti quegli automobilisti rispettosi della legge, che percorrono l'autostrada più lentamente.

Il risultato è che le velocità medie stanno aumentando, non diminuendo.

<<http://www.telegraph.co.uk/news/main.jhtml;sessionid=NRVAJJYZDVRXVQFIQMF?xml=/news/2005/04/25/ncam25.xml&sSheet=/portal/2005/04/25/%3Cbr%20/%3Eixportal.html>>

oppure <<http://tinyurl.com/7my9y>>

<<http://www.telegraph.co.uk/news/main.jhtml;sessionid=4BMMZNI41WICJQFIQMGCM5OAVCBQUJVC?xml=/news/2004/04/23/nspeed23.xml>> oppure <<http://tinyurl.com/7eoz9>>

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

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

I mandati come misure di sicurezza:

<<http://www.schneier.com/crypto-gram-0405.html#1>>

<<http://www.cryptogram.it/cryptogramPdf/Maggio2004.pdf>> (traduzione in italiano)

Consumatori della Sicurezza Nazionale:

<<http://www.schneier.com/crypto-gram-0405.html#9>>

<<http://www.cryptogram.it/cryptogramPdf/Maggio2004.pdf>> (traduzione in italiano)

Crittografia e intercettazioni telefoniche:

<<http://www.schneier.com/crypto-gram-0305.html#1>>

<<http://www.cryptogram.it/maggio03.htm#a1>> (traduzione in italiano)

Indirizzi e-mail specifici e Spam:

<<http://www.schneier.com/crypto-gram-0305.html#6>>

<<http://www.cryptogram.it/maggio03.htm#a6>> (traduzione in italiano)

Segretezza, Sicurezza e Oscurità:

<<http://www.schneier.com./crypto-gram-0205.html#1>>

<<http://www.cryptogram.it/maggio02.htm#a1>> (traduzione in italiano)

Ingannare i rilevatori di impronte digitali:

<<http://www.schneier.com./crypto-gram-0205.html#5>>

<<http://www.cryptogram.it/maggio02.htm#a5>> (traduzione in italiano)

Che cosa può insegnare alla Sicurezza della Rete la Storia Militare, Seconda Parte:

<<http://www.schneier.com/crypto-gram-0105.html#1>>

SSH, ovvero Secure SHell, è il protocollo standard per accedere in remoto a sistemi UNIX. Viene utilizzato ovunque: università, laboratori, aziende (specialmente in servizi di back office con grande traffico dati). Grazie a SSH, gli amministratori di rete possono accumulare centinaia di computer gli uni accanto agli altri in stanze con aria condizionata e amministrarli comodamente dall'ufficio.

Quando il client SSH di un utente stabilisce inizialmente il collegamento a un server remoto, archivia il nome del server e la sua chiave pubblica in un database `known_hosts`. Questo database di nomi e di chiavi permette al client di identificare più facilmente quel server in futuro.

Questo database, però, è soggetto a rischi. Se un aggressore compromette l'account dell'utente, il database può venire usato come elenco di host target da attaccare. E se l'aggressore conosce il nome utente, la password e le credenziali basilari dell'utente, è assai probabile che vengano accettate anche da questi host.

Un nuovo studio del MIT esamina le potenzialità che può avere un worm di utilizzare questo meccanismo di infezione per propagarsi in Internet. Già i vari aggressori stanno exploitando questo database dopo aver craccato password. Lo studio inoltre avverte che un worm che si propagasse attraverso SSH potrebbe benissimo eludere la gran quantità di tecniche di rilevamento messe in atto dalla comunità dei "cacciatori" di worm.

Se da un lato non si è ancora visto un worm di questo tipo dai tempi del primo worm in Internet del 1988, dall'altro gli attacchi si sono fatti sempre più sofisticati e la maggior parte dei tool necessari sono già nelle mani degli aggressori. È solo questione di tempo prima che qualcuno scriva un worm come questo.

Tuttavia è anche un worm semplice da sconfiggere. Una delle contromisure proposte nello studio è quella di archiviare nel database `known_hosts` gli hash dei nomi degli host, invece dei nomi stessi. Ciò è simile al modo con cui gli hash delle password vengono memorizzati nei database di password, così che la sicurezza non debba affidarsi completamente alla segretezza del database. Si risolve il problema della sicurezza senza perdita di funzionalità per l'utente.

Gli autori dello studio hanno lavorato insieme alla comunità open source, e la versione 4.0 di OpenSSH possiede l'opzione di "hashare" il database `known_hosts`. C'è anche una patch per OpenSSH 3.9 che svolge la stessa funzione. Purtroppo l'opzione non è attivata per default.

<<http://nms.csail.mit.edu/projects/ssh/>>
<<http://nms.csail.mit.edu/projects/ssh/sshworm.pdf>>

La soluzione:

<http://www.openbsd.org/cgi-bin/man.cgi?query=ssh_config>
<<http://www.openbsd.org/cgi-bin/man.cgi?query=ssh-keygen>>
<<http://www.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/hostfile.c?rev=1.34&content-type=text/x-cvsweb-markup>> oppure <<http://tinyurl.com/8938c>>

*** **

News

Rilevamento delle targhe automobilistiche effettuato via elicottero:

<<http://www.thenewspaper.com/news/03/320.asp>>

Questo è un esempio di sorveglianza su vasta scala, un argomento che ho già trattato in precedenza.

<<http://www.schneier.com/essay-061.html>>

Ovviamente, una volta che il sistema viene adottato, sarà usato per violare la privacy in modi che neanche immaginiamo. L'unica maniera per salvaguardare la sicurezza è non implementare affatto questo genere di sistemi.

Una revisione dell'eccellente studio a opera di Daniel Solove e Chris Hoofnagle che ha offerto proposte legislative specifiche per una riforma della privacy.

<http://papers.ssrn.com/sol3/papers.cfm?abstract_id=699701>

"A Taxonomy of Privacy" [Una tassonomia della Privacy], di Daniel Solove. Un lavoro davvero ottimo.

<http://papers.ssrn.com/sol3/papers.cfm?abstract_id=667622>

Altri fallimenti dello screening negli aeroporti:

<<http://www.cnn.com/2005/TRAVEL/04/16/airport.screeners.ap/>>

Trovate qui il mio commento:

<http://www.schneier.com/blog/archives/2005/04/failures_of_air.html>

Il Dipartimento per la Sicurezza Nazionale sta valutando tre diversi sistemi per processare i visti in uscita.

<<http://www.fcw.com/article88459-04-01-05-Web>>

Una valutazione appropriata di questo compromesso focalizzerebbe l'attenzione sulla relativa facilità di attaccare i tre sistemi, sui costi relativi dei tre sistemi, e la relativa velocità e comodità (per il viaggiatore) dei tre sistemi. A mio avviso il sistema migliore è quello che richiede la minor interazione con un essere umano quando ci si deve imbarcare sull'aereo.

Interessante articolo di giurisprudenza sulle responsabilità legate al possesso di una rete wireless aperta:

<http://papers.ssrn.com/sol3/papers.cfm?abstract_id=692881>

La sorveglianza automobilistica approda negli Emirati Arabi Uniti:

<<http://www.thenewspaper.com/news/03/328.asp>>

Un sistema del genere sta per essere implementato anche nel Regno Unito a scopi assicurativi:

<http://icnewcastle.icnetwork.co.uk/lifestyle/finance/tm_objectid=15392722&method=full&siteid=50081&headline=tracking-down-those-insurance-costs-name_page.html>

oppure <<http://tinyurl.com/6wmob>>

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

Un articolo davvero buono sui compromessi di sicurezza:

<<http://www.csoonline.com/read/040105/undercover.html>>

Due pinguini passano attraverso la security all'aeroporto:

<<http://www.thedenverchannel.com/slideshow/4402056/detail.html?qs=:s=1:w=320>>

oppure <<http://tinyurl.com/aju23>>

Formiche che organizzano agguati:

<<http://www.nature.com/news/2005/050418/full/050418-11.html>>

Il Dipartimento di Stato USA sta pensando di implementare il proprio passaporto RFID in maniera che sia richiesta una chiave master da un lettore prima che il passaporto trasmetta i dati in esso contenuti. Certo, il diavolo è nei dettagli, si dice, ma questa è un'idea eccellente.

<<http://www.wired.com/news/privacy/0,1848,67333,00.html>>

<http://www.schneier.com/blog/archives/2005/04/rfid_passport_s.html>

"The Emergence of a Global Infrastructure for Mass Registration and Surveillance" [L'Emergenza di una Infrastruttura Globale per la Registrazione e la Sorveglianza di Massa]: un rapporto molto interessante.

<<http://www.statewatch.org/news/2005/apr/icams-report.pdf>>

È una vecchia storia: gli utenti disattivano una misura di sicurezza perché è fastidiosa, permettendo così a un aggressore di aggirarla. "Un imputato accusato di stupro, in un'escalation di violenza con esito mortale è stato in grado di penetrare nell'ufficio del giudice, assassinarlo, e tenere gli occupanti in ostaggio perché la porta non era chiusa a chiave e il sistema di ingresso tramite interfono era disattivato", secondo il rapporto di uno sceriffo. La sicurezza non funziona finché non sono gli utenti a volere che funzioni. Questo è vero su scala personale e nazionale, con o senza tecnologia.

<<http://www.msnbc.msn.com/id/7423184>>

Ancora un altro fallimento nella redazione di un file PDF: questa volta si tratta di informazioni segrete in un rapporto statunitense sull'uccisione dell'agente segreto italiano Nicola Calipari in Iraq.

<<http://news.bbc.co.uk/go/em/fr/-/1/hi/world/europe/4504589.stm>>

<<http://vowe.net/archives/005838.html>>

<<http://www.livejournal.com/users/annafdd/110745.html>>

<http://story.news.yahoo.com/news?tmpl=story&cid=535&ncid=535&e=3&u=/ap/20050502/ap_on_re_eu/italy_us_iraq> oppure <<http://tinyurl.com/cq7y2>>

Un buon articolo riguardante le varie implicazioni del furto di dati a opera di ChoicePoint (e di tutti gli altri furti di dati, perdite e divulgazioni che fanno notizia).

<<http://www.csoonline.com/read/050105/choicepoint.html>>

Il Governo degli Stati Uniti sta considerando un'altra carica di capo della cyber-sicurezza, al Dipartimento per la Sicurezza Nazionale. Purtroppo non servirà a niente. Certo, è una buona cosa avere un funzionario di livello superiore a cui affidare la cyber-sicurezza, ma una responsabilità senza autorità non porta a nulla. Un altro pulpito ancora più altisonante e borioso non apporterà alcun beneficio senza un piano coerente dietro, e non abbiamo alcun piano. La cosa migliore in assoluto che il Dipartimento per la Sicurezza Nazionale potrebbe fare per la cyber-sicurezza sarebbe quella di coordinare l'enorme potere di acquisto del Governo degli Stati Uniti e richiedere hardware e software più sicuri.

<http://www.infoworld.com/article/05/04/20/HNhousesecurity_1.html>

<<http://www.govtrack.us/congress/billtext.xpd?bill=h109-285>>

Un buon articolo sul furto d'identità:

<<http://members.optusnet.com.au/paul.mcgowan/phishing.html>>

Un'azienda persiste nel mantenere cattive pratiche in merito alla sicurezza delle informazioni:

<<http://www.baltimoresun.com/business/bal-bz.safenet05may05,1,3741390.story>>

Il mio commento:

<http://www.schneier.com/blog/archives/2005/05/company_continu.html>

Anche The Onion parla di furti d'identità:

<<http://www.theonion.com/news/index.php?issue=4118>>

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

Passaporti biometrici nel Regno Unito

Il Governo Britannico ha cercato di istituire un documento d'identità nazionale, senza successo. Adesso vuole aggiungere dati biometrici al passaporto. Secondo il rapporto: "I finanziamenti a favore dell'Ufficio Passaporti aumenteranno da 182 milioni di sterline l'anno a 415 milioni di sterline entro il 2008, per far fronte all'introduzione di informazioni biometriche come le impronte digitali. Un portavoce del Ministero degli Interni ha dichiarato che lo scopo è quello di eliminare le 1.500 istanze fraudolente scoperte attraverso il sistema postale lo scorso anno".

Nel caso delle normali mine terrestri, ogni controllo umano viene escluso non appena posa la mina. Persino un 19enne che vede un puntino intermittente su uno schermo è migliore di un sistema completamente automatizzato.

Se io fossi l'esercito degli Stati Uniti, sarei più preoccupato dall'eventualità che le mine possano essere innescate accidentalmente da interferenze radio. Sarei più preoccupato dalla possibilità che il nemico usi dei jammer per disturbare il sistema di radiocontrollo.

<http://www.usatoday.com/tech/news/2005-04-12-laptop-mines_x.htm>

<<http://www.theinquirer.net/?article=22522>>

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

Il Rapporto PITAC sulla Cyber-sicurezza

Sono finalmente riuscito a leggere il rapporto PITAC (President's Information Technology Advisory Committee) dal titolo "Cyber Security: A Crisis of Prioritization" [Cyber-sicurezza: una crisi di prioritizzazione], datato febbraio 2005. Il rapporto esamina lo stato attuale del coinvolgimento federale nella ricerca in ambito di cyber-sicurezza, e stila una serie di indicazioni per il futuro. È un ottimo rapporto, un rapporto che l'amministrazione farebbe bene a seguire.

Le indicazioni del rapporto si basano su due osservazioni: 1) la ricerca sulla cyber-sicurezza si incentra primariamente su minacce attuali e non a lungo termine; 2) non ci sono abbastanza ricercatori sulla cyber-sicurezza, e manca un buon sistema per produrne di nuovi. Il governo federale non si sta muovendo molto per incoraggiare la ricerca sulla cyber-sicurezza, e gli effetti di questo calo inaspettato si faranno maggiormente sentire sul lungo termine, non a breve.

Per rimediare a tale problema, il rapporto enuclea quattro indicazioni specifiche (in maniera molto più dettagliata di quanto da me riportato qui). Uno - il governo deve aumentare i finanziamenti a favore di una ricerca di base sulla sicurezza cibernetica. Due - il governo deve aumentare il numero di ricercatori che lavorano in ambito di sicurezza cibernetica. Tre - il governo deve maggiormente incentivare il trasferimento di tecnologia dalla ricerca allo sviluppo del prodotto. Quattro - il governo deve migliorare il proprio coordinamento e supervisione in ambito di sicurezza cibernetica. Quattro ottime indicazioni.

Più specificamente, il rapporto elenca dieci tecnologie a cui serve maggiore ricerca. Esse sono (senza un ordine particolare di priorità):

- Tecnologie di autenticazione
- Protocolli sicuri fondamentali
- Secure Software Engineering e Software Assurance
- Sicurezza olistica dei sistemi
- Monitoring e rilevamento
- Metodologie di mitigazione e di recupero
- Cyber Forensics
- Progettazione e banchi di prova per nuove tecnologie
- Metrica, Benchmark e Best Practice
- Problematiche non legate alla tecnologia che possono compromettere la sicurezza cibernetica

È un buon elenco, e in special modo mi fa molto piacere veder elencato il decimo elemento, che viene solitamente dimenticato. Aggiungerei qualcosa del tipo "Sistemi di cyber-sicurezza dinamici", poiché ritengo che sia necessaria una ricerca di base su come i sistemi dovrebbero reagire a nuove minacce e come aggiornare la sicurezza di sistemi già installati. Ma sarebbe l'unica cosa che aggiungerei.

Il rapporto, in se stesso, è un po' ripetitivo, ma vale davvero la pena di essere consultato.

<http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf>
oppure <<http://tinyurl.com/79vj6>>

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

Furto d'identità sponsorizzato dallo Stato

Nel corso di un'operazione di copertura a uno strip bar nell'Ohio, una studentessa di 22 anni, un interno dell'U.S. Marshal Service, ha ricevuto una falsa identità in modo da poter lavorare sotto copertura al locale. Però, invece di assegnarle un'identità totalmente fittizia, la polizia le ha dato quella di un'altra donna di un'altra cittadina dell'Ohio. E quest'altra donna non è stata nemmeno informata della cosa.

Per quanto strano, tutto ciò è legale. Secondo la legge dello stato dell'Ohio sul furto d'identità, la polizia ha il permesso di farlo. Il furto d'identità non può essere perseguito se: "La persona o entità che utilizza le informazioni personali di identificazione è un'agenzia delle forze dell'ordine, un membro autorizzato dell'antifrode, o un rappresentante o il legale di un'agenzia delle forze dell'ordine o di un membro autorizzato dell'antifrode e si sta servendo delle informazioni personali di identificazione nel corso di un'indagine in buona fede, una verifica di information security, un pretesto che richieda una certa verifica, o questioni simili".

Devo ammettere di essere sbalordito. Supponevo ingenuamente che la polizia avesse un elenco di numeri di Previdenza Sociale riservati, da poter utilizzare in casi come questo. O, almeno, che usasse le identità di persone di altre parti del paese e solo dopo aver richiesto un permesso (sono certo che non mancherebbero volontari per aiutare la polizia). Non avrei mai pensato che arrivasse a rubare l'identità di cittadini presi a caso. Ma che cosa gli passa per la testa?

<<http://www.officer.com/article/article.jsp?siteSection=5&id=22852>>

La legge dell'Ohio:

<http://www.legislature.state.oh.us/bills.cfm?ID=126_HB_48>

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

Combattere lo Spam

Lo spam torna a far parlare di sé, con un nuovo nome. Stavolta si tratta di spam voice-over-IP, e viene indicato col simpatico nomignolo di "spit" (Spam Over Internet Telephony, ovvero Spam tramite la telefonia via Internet). Spit ha il potenziale di devastare completamente il VoIP. Nessuno installerà tale sistema se la prospettiva è ricevere decine di chiamate al giorno da parte di spammer audio, o quantomeno di dover accettare solo quelle chiamate provenienti da una white list di chiamanti fidati.

Lo spam VoIP va ad aggiungersi alle già note categorie di spam via e-mail, di spam via newsgroup di Usenet, di spam via Instant Messaging, di spam degli SMS dei cellulari e di spam nei commenti dei blog. E, se ragioniamo per estensione, questi meccanismi di distribuzione dello spam attraverso reti di computer vanno ad aggiungersi alle categorie di telemarketing elettronico (spam telefonico), della posta indesiderata (spam cartaceo), dei cartelloni pubblicitari (spam dello spazio visivo) e delle auto con megafono che girano in città facendo pubblicità (spam sonoro). Si tratta fondamentalmente della stessa cosa -- messaggi pubblicitari

indesiderati -- e soltanto capendo il problema a questo livello generale possiamo provare a parlare di soluzioni.

In generale, lo scopo della pubblicità è quello di influenzare le persone. Di solito si spingono le persone ad acquistare un prodotto, ma è anche possibile spingerle a sostenere un certo candidato in politica o una certa posizione. La pubblicità fa questo inculcando un messaggio di marketing nella mente del destinatario. Il meccanismo di tale "instillazione" è semplicemente una tattica, una strategia.

Le varie tattiche con cui veicolare messaggi pubblicitari indesiderati acquistano e perdono in popolarità a seconda dei loro costi/benefici. Se i benefici sono significativi, si investirà più denaro. Se il beneficio è minimo, la cosa verrà messa in atto solo se è a buon mercato. Uno spot televisivo di 30 secondi in prima serata costa 1,8 cent per singolo spettatore adulto; una pubblicità a colori a tutta pagina su una rivista costa 0,9 cent per lettore. Un cartellone pubblicitario collocato in autostrada costa 0,21 cent per automobile. Il Direct Mailing è il più caro, costando più di 50 cent per lettera ordinaria inviata (ecco perché intere mailing list da bersagliare sono così preziose: aumentano il beneficio per singola unità).

Lo spam è una tattica così diffusa non perché sia particolarmente efficace; infatti, i tassi di risposta allo spam sono molto bassi. È diffuso perché è mostruosamente a basso costo. In genere gli spammer chiedono meno di 1/100 di cent per e-mail (e questa cifra si riferisce solo a quanto chiedono le società di spamming ai propri clienti per distribuire lo spam; se siete dei bravi hacker potete costruirvi la vostra rete di spam personale per molti meno soldi). Se per voi riuscire ad influenzare con successo una persona (a comprare il vostro prodotto, a votare per il vostro candidato, ecc.) vale 10 dollari, allora vi basta un tasso di successo pari a 1 su 100.000. Con lo spam si possono commercializzare prodotti davvero marginali.

Fin qui tutto bene. Ma il calcolo costi/benefici manca di una componente: il "costo" di infastidire la gente. Tutti coloro che non vengono influenzati dal messaggio pubblicitario vengono infastiditi in varia misura. L'inserzionista paga un costo parziale per scocciare le persone: il rischio che queste possano boicottare il suo prodotto. Ma nella maggior parte dei casi questo costo non viene pagato e ricade sulla persona: la bellezza del paesaggio è guastata dal cartellone, la cena è interrotta da un venditore che chiama al telefono, lo spam costa denaro per muoversi attraverso Internet e tempo per procedere faticosamente, eccetera. Si noti come io stia usando il termine "costo" in senso generico, e non necessariamente in senso monetario. Il tempo e la felicità sono entrambi dei costi.

E questo è il motivo per cui lo spam è così negativo. Per ogni e-mail, lo spammer paga un costo e ottiene un beneficio. Ma c'è un costo aggiuntivo che viene pagato dal destinatario dell'e-mail. Dato che moltissimo spam è indesiderato, il costo aggiuntivo è enorme, ed è un costo che lo spammer non vede mai. Se si potesse far gravare il costo totale dello spam sugli stessi spammer, allora il livello di spam sarebbe più vicino a quel che la società trova accettabile.

Questa analisi economica è importante, perché è l'unico modo per comprendere in che misura possano essere efficaci varie soluzioni. Si tratta di un problema economico, ed è necessario che le soluzioni modifichino gli aspetti fondamentali di questa economia. L'analisi è grosso modo la stessa per lo spam VoIP, per lo spam attraverso i newsgroup di Usenet, per lo spam dei commenti nei blog, e così via.

Le soluzioni migliori aumentano i costi per lo spam. I filtri anti-spam aumentano il costo perché fanno aumentare la quantità di spam che uno deve inviare prima che un destinatario abbia modo di leggerlo. Se il 99% dello spam viene filtrato e cestinato, allora inviare dello spam diventa 100 volte più costoso. Questo è anche il principio che sottende le cosiddette white list (lett. "liste bianche", ossia elenchi di mittenti dai quali accettare messaggi e-mail) e le black list (lett. "liste nere", ovvero elenchi di mittenti i cui messaggi e-mail non verranno accettati).

Il filtro non deve essere necessariamente posto al livello dell'e-mail del destinatario. Può essere implementato all'interno di una rete allo scopo di rigettare lo spam, o al livello del mittente. Parecchi ISP stanno già filtrando la posta in uscita per evitare lo spam, e questa tendenza aumenterà.

Leggi anti-spam innalzano il costo dello spam a livelli intollerabili; a nessuno fa piacere andare in galera per spamming. Si sono già viste alcune condanne negli Stati Uniti. Sfortunatamente questo funziona soltanto quando lo spammer è effettivamente entro la portata della legge, ed è meno efficace contro quei criminali che si servono dello spam come sistema per commettere frodi.

Altre soluzioni proposte cercano di imporre costi diretti sulle spalle di chi invia e-mail. Ho visto proposte di "affrancatura elettronica" sulle e-mail, per ogni e-mail inviata oppure per ogni e-mail spedita oltre una soglia ragionevole. Ho visto proposte secondo cui il mittente di una e-mail invia una piccola cauzione, che il destinatario può incassare se l'e-mail è spam. Vi sono altre proposte che comportano "puzzle computazionali": rompicapi che il computer del mittente deve svolgere, del tutto trascurabili se si inviano messaggi e-mail normalmente, ma assolutamente onerosi per chi invia un gran numero di e-mail per volta. Queste soluzioni di solito implicano una reingegnerizzazione di Internet, una cosa che non può esser fatta con leggerezza, e di qui il motivo per cui sono ancora ferme allo stadio di dibattito.

Tutte queste soluzioni funzionano in una certa misura, e si finisce con l'instaurare un braccio di ferro. I prodotti anti-spam bloccano un certo tipo di spam. Gli spammer inventano una strategia per aggirare questi prodotti. Poi i prodotti bloccano anche quel nuovo tipo di spam. Poi gli spammer inventano ancora un altro genere di spam. E così via.

Mettere in una black list i siti degli spammer ha costretto gli spammer a camuffare l'origine dei messaggi e-mail di spam. Le persone che hanno cominciato a riconoscere i messaggi di mittenti fidati, e altre misure anti-spam, hanno costretto gli spammer a penetrare in macchine innocenti e ad usarle come piattaforme di lancio. La scansione di milioni di messaggi e-mail alla ricerca di gruppi identici di spam ha costretto gli spammer a rendere originale ogni messaggio. La rilevazione semantica dello spam ha costretto gli spammer a ideare metodi di spam sempre più furbi. E via dicendo. Ad ogni difesa risponde un attacco, e ad ogni attacco si risponde con una nuova difesa.

Ricordatevi di questo quando pensate all'identificazione dell'host o all'"affrancatura" come tattiche anti-spam. Agli spammer non importano le tattiche: a loro interessa spedire e-mail. Tecniche come queste finiranno semplicemente con lo spingere gli spammer ad affidarsi sempre più a macchine innocenti violate. Finché i computer sottostanti sono insicuri, non possiamo impedire agli spammer di inviare posta.

Questo è il problema legato ad un'altra soluzione potenziale: reingegnerizzare Internet per proibire la falsificazione degli header dell'e-mail. Ciò semplificherebbe il lavoro del software anti-spam nella rilevazione degli indirizzi IP da cui proviene lo spam, ma gli spammer continuerebbero a usare computer violati invece dei propri.

In tutta onestà, non si vede una fine di questo eterno braccio di ferro con lo spam. Attualmente, l'80-90% dei messaggi e-mail sono spam, e la percentuale è in aumento. Sono eternamente alle prese con lo spam nei commenti al mio blog. Però malgrado tutto, lo spam è una di quelle storie che vede la sicurezza informatica riuscire vittoriosa. L'attuale insieme di prodotti anti-spam funziona piuttosto bene, se le persone hanno voglia di impegnarsi per configurarli. Io non ricevo quasi più spam, e pochissime e-mail legittime sono vittima dei miei filtri anti-spam. Mi piacerebbe che funzionassero meglio (Crypto-Gram viene occasionalmente bollata come spam da alcuni ISP, per esempio), ma tutto sommato non posso lamentarmi. Ci vorrà ancora molto tempo prima che lo spam smetta di intasare Internet, ma almeno abbiamo delle tecnologie che ci permettono di non doverlo vedere.

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

Commenti dei lettori

Da: Keith Martin <keith@keith.gs>

Oggetto: Attenuare il problema del furto d'identità

In Europa (e in Irlanda in special modo) abbiamo delle regole piuttosto estese per gestire ciò a cui lei si riferisce dicendo "attivare una carta di credito semplicemente riempiendo un modulo di informazioni". Esiste un requisito legale per ogni banca o compagnia di carta di credito in Irlanda che ha lo scopo di verificare l'identità di chi richiede un conto bancario o una carta di credito, e si utilizzano (almeno) due metodi distinti.

Uno, per esempio, è di solito un documento identificativo con fototessera. I più comuni sono il passaporto o la patente di guida (molti irlandesi possiedono un passaporto, ma non so se questa opzione funzionerebbe negli USA), e l'altro è la dimostrazione di un indirizzo veritiero (per esempio presentando una bolletta telefonica o qualsiasi altra bolletta). È sicuramente possibile ottenere l'uno o l'altro documento, ma più difficile ottenerli entrambi. Inoltre, la bolletta non deve essere più vecchia di sei settimane, per cui si limita (anche se non la si elimina del tutto) la possibilità di utilizzare vecchi indirizzi o indirizzi falsi.

Non è sicuro al 100%, ma è migliore di alcuni sistemi usati in altri paesi. La legislazione fu originariamente introdotta per evitare il riciclaggio di denaro sporco, ma con un utile doppio scopo, a cui i legislatori non avevano pensato all'inizio (di questo sono certo, visto che l'ho esplicitamente chiesto a loro!).

Da: Charles H Baker <chb@charleshbaker.com>

Oggetto: Attenuare il problema del furto d'identità

Una cosa che vorrei portare alla sua attenzione è che dal momento in cui il FACTA entrerà in vigore il primo giugno, i consumatori diventeranno responsabili per le transazioni fraudolente nel caso non informino l'istituzione finanziaria entro 60 giorni (30 in alcuni casi). Questo è davvero un problema perché molte delle vittime non si rendono conto di essere tali prima che sia passato un anno o più (secondo statistiche dell'FTC).

Inoltre, l'FTC dichiara che solo il 26% dei furti d'identità è di tipo finanziario. Il resto sono frodi ai danni della sanità, del fisco, ecc. Come potrebbe essere una soluzione l'autenticare una transazione se qualcuno utilizza il mio numero di Previdenza Sociale per ottenere un posto di lavoro e poi non paga le tasse? L'IRS verrà a cercare me!

Da: Andrew Blank <andrew.blank@wanadoo.nl>

Oggetto: Attenuare il problema del furto d'identità

Lei ha assolutamente ragione nell'affermare, nei suoi recenti numeri di Crypto-Gram, che l'autenticazione della transazione (e non dell'utente) è il punto chiave nelle transazioni finanziarie. Gli olandesi sono con lei. Ecco come funziona da qualche anno l'Internet Banking qui in Olanda.

1. I clienti di una banca possiedono delle tessere Bancomat con un chip in cui viene memorizzato il loro PIN.

2. I clienti del banking online possiedono un token: un "calcolatore" di tipo challenge-response (richiesta-risposta). Il calcolatore non è unico per il singolo individuo, ma ogni calcolatore deve

essere sbloccato inserendo la tessera Bancomat e digitando il PIN. Questo fa in modo che il calcolatore venga personalizzato per l'utente, per tutto il tempo in cui la tessera è inserita. Una volta sbloccato, il calcolatore andrà in stop dopo alcuni minuti, e per essere "risvegliato" richiederà nuovamente il PIN.

3. Gli utenti si autenticano per effettuare il banking online sul Web inserendo il loro numero di conto e il numero di serie (non il PIN, ovviamente) della loro tessera Bancomat. La banca emette una richiesta (8 digit) che l'utente immette nel calcolatore e risponde utilizzando la risposta a 6 digit fornita dal computer.

4. A questo punto l'utente ha accesso al conto, e può preparare (ma non spedire) i vari pagamenti. In genere l'utente emette pagamenti verso conti correnti già inseriti nel suo indirizzario bancario. Ogni nuova voce in questo indirizzario genera un meccanismo di richiesta-risposta da parte della banca (e questo probabilmente significa anche che l'utente deve reinserire il suo codice PIN per "svegliare" il proprio calcolatore). Se un utente effettua un grosso pagamento verso un conto corrente che non figura nell'indirizzario, allora viene attivato un altro impulso richiesta-risposta per convalidare i dettagli del conto ricevente.

5. Infine, quando tutti i pagamenti sono stati preparati e messi in ordine, l'utente seleziona il pulsante "Inviare alla banca". Un elenco di tutte le transazioni in coda (beneficiari e somma da pagare) viene visualizzato e un ultimo impulso richiesta-risposta è necessario per confermare l'invio del gruppo di pagamenti.

Il sistema non è perfetto, ma sembra piuttosto buono. Dà del filo da torcere a qualsiasi attacco man-in-the-middle perché diventa difficile inventare un pagamento e convincere in qualche modo l'utente ad autenticare una transazione non originata da lui medesimo. Ovviamente l'utente ha a che fare con operazioni un po' più laboriose del solito, ma in cambio ottiene la certezza che è lui, e non qualche estraneo, ad essere padrone del proprio denaro.

Da: Andy Clark <andy.clark@dial.pipex.co.uk>

Oggetto: Attenuare il problema del furto d'identità

In riferimento alla responsabilità per frodi ai danni della carta di credito, le cose stanno cambiando nel Regno Unito con l'introduzione del sistema chip and PIN. Quando effettuiamo delle transazioni, la carta deve essere inserita in un dispositivo e occorre digitare un PIN. Una buona cosa di questo sistema è che la carta non abbandona mai la persona che sta effettuando la transazione; per il conto del ristorante, ad esempio, il dispositivo per il pagamento viene solitamente portato al tavolo del cliente.

Oltre a questo, la maggior parte delle compagnie di carte di credito sta modificando i propri termini e condizioni contrattuali per far ricadere la responsabilità sul possessore della carta e anche per responsabilizzarlo in merito alla sicurezza della propria carta e del proprio PIN. Prima, se a qualcuno veniva rubata una carta di credito e il furto segnalato entro un'ora, il possessore della carta era responsabile solo dei primi 50 dollari; adesso è responsabile per tutte le transazioni effettuate in quell'ora.

Come esempio, si vedano alcuni termini e condizioni di carte di credito britanniche:

<<http://www.firstdirect.com/legals/creditcard.shtml>>

<<http://www.barclaycard.co.uk/Products/Apply/tandc.html>>

Da: laszlo@hars.us

Oggetto: Attenuare il problema del furto d'identità

Negli anni Ottanta e nei primi anni Novanta ho vissuto in Germania. Il sistema bancario tedesco era molto più evoluto allora di quanto lo sia adesso negli Stati Uniti. Tutte le mie bollette, fatture, polizze, ecc., venivano automaticamente detratte dal mio conto (dopo una mia unica autorizzazione scritta) e avevo sei settimane a disposizione per annullare qualsiasi addebito per qualsiasi motivo. Non dovevo scrivere nessun assegno; qualsiasi attività criminale sarebbe stata ben più sospetta. L'uso di carte con chip come tessere Bancomat e la mia VISA con la mia foto sulla parte frontale erano altre piccole aggiunte alla sicurezza generale.

Quasi vent'anni fa il livello di sicurezza era ben più alto laggiù che non qui negli USA oggi. La mia banca mi fornì una lista di numeri TAN per autenticare le transazioni, ognuno di essi da usarsi una volta sola. Per il banking online dovevo autenticarmi con la solita procedura nome utente/passphrase e dovevo anche fornire un numero di transazione preso dall'elenco stampato. Nessun software maligno poteva entrare nel cassetto della mia scrivania per prendere quell'elenco. Anche fare una fotocopia dell'elenco di nascosto era di poca utilità, perché me ne sarei accorto inserendo il numero TAN successivo. Uno spoofing online del TAN o attacchi man-in-the-middle avrebbero permesso a un malintenzionato di modificare un'unica transazione, ma la cosa non sarebbe sfuggita al legittimo correntista: la sua transazione non va a buon fine o non produce i conteggi finali che ci si aspetta. Una telefonata avrebbe evitato qualsiasi danno.

Il problema negli Stati Uniti è che esiste una tale competizione per accaparrarsi nuovi clienti che anche il loro più piccolo fastidio (come inserire un numero di transazione e segnarlo come utilizzato) potrebbe portare alla perdita di qualche cliente. È una semplice equazione: se un sistema bancario molto facile da usare attrae più clienti, e il profitto extra che ne deriva è maggiore di quanto la banca si aspetta di perdere a causa di frodi, allora il sistema semplice ma non sicuro verrà usato; e a maggior ragione se le banche possono far gravare le perdite sui clienti stessi o sui commercianti. Come lei dice, la soluzione è quella di rendere le istituzioni finanziarie responsabili per le transazioni fraudolente.

Da: John <atfdjsj02@sneakemail.com>

Oggetto: Attenuare il problema del furto d'identità

Sono uno dei senior technical architect dello staff di un punto vendita di una catena retail nazionale, e posso assicurarle che conosco molto bene i procedimenti di autorizzazione di credito e di liquidazione.

Il credito funziona così: se otteniamo un'autorizzazione di credito positiva da parte di Visa (quell'"auth code" che si vede stampato sulle ricevute ne è la prova), allora vuol dire che Visa ha assunto la responsabilità per la transazione, e noi veniamo pagati mediante un processo chiamato liquidazione.

Vi sono svariati collegamenti di rete attraverso cui una richiesta di autorizzazione viaggia dal POS alla filiale Visa emittente (e ritorno). Nulla è perfetto, e talvolta i sistemi di autorizzazione del credito vanno offline. In tal caso il nostro call center processa le richieste di autorizzazione via telefono (in genere vengono gestite domande sui conti correnti, fatturazioni e/o solleciti, o chiamate di autorizzazione per carte che possono richiedere un'ulteriore fase di processazione). Ma tutta questa processazione via telefono è molto costosa in termini di tempo perso dal cassiere e di frustrazione del cliente, per non parlare del carico aggiunto che grava sul personale del call center, per cui abbiamo quel che viene chiamato "limite minimo" -- una qualunque addebito offline sotto questo limite viene automaticamente approvata dalla nostra società. Questo significa che ci siamo assunti la responsabilità per quell'addebito.

In genere il limite minimo è irrilevante -- siamo online per il credito più del 99% del tempo. Ma quando siamo davvero offline, il valore di quel limite agisce da valvola per il call center. Se abbiamo il limite impostato a 1,00 dollari, potremmo avere un migliaio di chiamate al minuto. E se lo portiamo a 10.000,00 dollari potremmo avere una chiamata all'ora. Quindi variamo quel

limite basandoci sul rischio che intendiamo correre di contro alla capacità del nostro call center di gestire le chiamate in una situazione in cui siamo offline.

Se ci assumiamo la responsabilità per una transazione nel caso in cui siamo offline per Visa, e in seguito c'è qualche problema con quella transazione (il cliente lamenta un utilizzo fraudolento, o si rifiuta di pagare) allora Visa emette un "chargeback" a noi e ci accolliamo la perdita. Niente "auth code", nessun pagamento. Inutile dire che è considerato molto importante mantenere i sistemi online per evitare un simile rischio.

È anche importante mantenere segreto il valore corrente del limite minimo perché le notizie sui guasti dei sistemi si diffondono in fretta tra i criminali; individui con carte di credito fasulle o fraudolente o carte relative a conti chiusi o illegali arriverebbero a frotte nei nostri negozi se sapessero che siamo offline. La certezza che possono spendere impunemente 7,99 dollari di contro a vedersi rifiutato un addebito di 8,00 dollari porta a un mucchio di piccole transazioni fraudolente. Il problema non è così drammatico in caso di guasti temporanei o intermittenti, ma in uno scenario più grave (come dopo gli uragani che hanno colpito la Florida) siamo facilmente sopraffatti. Dopo aver ripristinato l'energia elettrica e un qualche servizio telefonico (un cellulare funzionante è considerato adeguato), nella lista delle priorità segue immediatamente l'esigenza di avere sufficiente banda per le autorizzazioni di credito online.

Inoltre, non siamo l'unico anello nella catena delle autorizzazioni. Per esempio, non abbiamo linee dirette con tutte le banche affiliate a Visa. Ci affidiamo a un servizio unificatore di terze parti in modo che agisca da nostro gateway nel network Visa. E anche questo servizio impiega dei limiti minimi per controllare il volume nei loro sistemi. Se si fanno carico dell'autorizzazione Visa, allora possiamo reindirizzare a loro i nostri chargeback, dato che loro sono gli unici ad essere ritenuti responsabili nei nostri confronti per qualsiasi transazione fraudolenta da loro approvata.

Lo stesso sistema viene adeguato anche al Mom & Pop's store, dove hanno un terminale Verifone per l'autorizzazione dei crediti. Se ottengono un auth code dal loro servizio di autorizzazione Visa, allora vengono pagati. Se passano la vostra carta su una impressionatrice vecchio tipo e non fanno una telefonata, allora non verranno pagati per un addebito fraudolento. Ma se chiamano e scrivono l'auth code sul talloncino senza carta copiativa e fanno un'impressione della carta per verificare la sua presenza, allora vengono pagati. È nel loro contratto.

Per la maggior parte dei casi le compagnie di carte di credito si accollano le perdite. È una delle ragioni per cui chiedono tassi d'interesse esorbitanti -- per coprire i propri rischi.

Da: Anton Holzherr <anton@holzherr.ch>

Oggetto: Attenuare il problema del furto d'identità

L'autenticazione della transazione (o la mancanza di essa) non è soltanto un problema legato all'e-commerce. In Svizzera i giornali hanno parlato di ripetuti abusi ai danni dei sistemi di pagamento bancari, dove pagamenti effettuati dai clienti della banca per posta ordinaria sono stati illecitamente dirottati verso altri conti correnti. Si veda ad esempio:

<<http://www.beo-news.ch/BNS2004/nov2004/klau17.htm>>

In Svizzera, i pagamenti dei vari debiti non vengono eseguiti come negli Stati Uniti inviando un assegno per coprire la richiesta di pagamento di un creditore. Qui funziona al contrario. Ogni creditore invia, insieme alla sua fattura, uno scontrino di deposito che contiene i dettagli del suo conto corrente e un numero di riferimento. Con queste informazioni, il debitore emette un ordine di pagamento alla banca, recandosi allo sportello, servendosi di una transazione sicura in Internet, o inviando un ordine di pagamento via posta ordinaria.

Di regola, il sistema di pagamento per posta normale utilizza l'autenticazione soltanto per la somma totale di tutte le transazioni contenute in un blocco di pagamenti. Riassumendo: alla fine del mese il signor Rossi raccoglie tutti i cedolini di pagamento di tutti i suoi creditori, fa il totale di tutte le richieste di transazione, compila un ordine di pagamento globale per la banca dove viene riportato questo totale, firma e invia alla banca questo ordine di pagamento, insieme a tutti i cedolini, in una busta sigillata.

I ladri rubano questi ordini di pagamento (cartacei) in piena notte. Servendosi di chiavi duplicate, ganci o nastro adesivo, pescano le lettere estraendole dalle cassette con la posta in uscita. Poi vi sostituiscono i propri cedolini di deposito, accertandosi che il totale coincida, e quindi dirottano il denaro verso i loro conti correnti. Il cliente della banca scopre l'inganno solo alla fine del mese successivo, quando riceve l'estratto conto e si accorge che i suoi soldi non sono andati ai suoi creditori ma a qualcun altro.

Questa frode funziona perché le banche richiedono solo una firma legale che autentichi la somma totale, e non una firma per ogni transazione effettuata.

Quello che i giornali non dicono è come facciano a rimanere anonimi i criminali che dirottano il denaro verso i propri conti.

Da: Joseph K Huffman <Joseph.Huffman@pnl.gov>
Oggetto: Accendini banditi sugli aeroplani

Gli esplosivi sono un mio hobby. Ho una regolare licenza ATFE per realizzare esplosivi di grosso calibro. Lo faccio abbastanza spesso, a scopo ricreativo.

Ho creato gli esplosivi per un evento recente utilizzando dei guanti. Ho dovuto poi sistemare alcune cosette in un secondo momento e li ho maneggiati senza guanti. Pochi minuti dopo ho maneggiato la custodia di un fucile dimenticandomi di pulirla. Il 13 aprile, tre giorni dopo, quella stessa custodia di fucile ha passato la security all'aeroporto Pasco Washington. Ho osservato un agente della TSA pulire la maniglia e l'interno della custodia e sottoporli al test per gli esplosivi. Tutto è passato senza problemi. La custodia del fucile mi ha seguito ad Albuquerque, New Mexico. Il 16 aprile quella stessa custodia ha fatto il viaggio di ritorno ed ha superato lo screening della TSA senza obiezioni. Di storie come questa ne ho tante; questa è solo la più recente.

Per quanto mi è dato vedere, la "sicurezza" negli aeroporti esiste solo per fare che la gente si senta meglio. Non rappresenta un deterrente nemmeno per un avversario dalle modeste capacità. Stiamo buttando via qualcosa come 1,8 miliardi di dollari all'anno su queste cose solo per fare in modo che certa gente si senta meglio.

Da: "Mike Glendinning" <mikeg@dulciana.com>
Oggetto: L'autenticazione a due canali con cellulari e SMS

Nel numero di marzo di Crypto-Gram, lei ha scritto in merito all'uso di un meccanismo di autenticazione "a due canali", usato da una banca, che aveva a che fare con telefoni cellulari e SMS. A questa tecnica viene dato ulteriore appoggio nel numero di aprile con l'intervento di Jonathan Tuliani.

Mi sembra tuttavia doveroso fare un piccolo richiamo alla cautela. In qualità di consulente per l'industria delle telecomunicazioni, in passato ho progettato svariati sistemi che facevano uso di questa tecnica, ma credo che stia diventando rapidamente molto meno utile. Tale tecnica parte dal presupposto che il network cellulare sia chiuso, ben controllato, e che in particolar modo

racchiuda sia l'origine del messaggio (ad esempio la banca) sia il cellulare dell'utente. Ma tre trend tecnologici nell'industria delle telecomunicazioni fanno cadere questo assunto di base:

1) L'industria dei cellulari si sta allontanando dall'uso di protocolli proprietari a livello di network per la distribuzione di servizi quali lo SMS. Per esempio, il più recente Multimedia Messaging Service (MMS) si basa su protocolli Internet aperti come l'HTTP. Le nozioni necessarie alla creazione e allo spoofing dei messaggi si sta perciò diffondendo sempre più.

2) I network chiusi e sicuri offerti dalle aziende di telecomunicazioni si stanno aprendo e vengono interconnesse a Internet per offrire l'esperienza "Web senza fili" e servizi di messaggistica di terze parti. Di conseguenza questi network non rappresentano più un canale completamente distinto e indipendente rispetto a Internet. La creazione di messaggi sta diventando sempre più facile, poiché non richiede più una connessione specializzata e dedicata all'azienda di telecomunicazioni.

3) Le vecchie apparecchiature telefoniche "non intelligenti", dove il software è completamente controllato dal produttore e dall'operatore di rete, vengono ora rimpiazzate da dispositivi "intelligenti" totalmente programmabili dall'utente finale. Ora esistono diverse possibilità di realizzare trojan e attacchi man-in-the-middle da parte di applicazioni maligne che girano sul telefonino stesso. Ad esempio, usando smartphone dotati del sistema operativo Symbian (e, in minor misura, Java/J2ME) è possibile per tali applicazioni intercettare tutti gli SMS in arrivo, non che avere pieno controllo dell'interfaccia utente.

Come si può vedere, sta diventando al tempo stesso più semplice iniettare messaggi falsi nel meccanismo di autenticazione "a due canali" e intercettare i messaggi veri. Purtroppo ho l'impressione che in molti nell'industria delle telecomunicazioni non abbiano inteso appieno queste problematiche, così come non sono state capite da coloro che si affidano a questa tecnologia ai fini dell'autenticazione utente.

Suppongo che la morale sia che è importante comprendere con chiarezza tutte le assunzioni su cui si basa qualsiasi meccanismo di sicurezza. E che tali assunzioni debbano essere continuamente riviste e ri-verificate nell'ottica di un contesto in continuo cambiamento.

** *** *****

CRYPTO-GRAM è una newsletter mensile gratuita che offre riassunti, analisi, approfondimenti, e commenti sulla sicurezza (informatica e in generale) e sulla crittografia. I numeri arretrati sono disponibili all'indirizzo <<http://www.schneier.com/crypto-gram.html>>.

Per iscriversi, cancellare l'iscrizione o cambiare il proprio indirizzo a cui recapitare la newsletter, visitate: <<http://www.schneier.com/crypto-gram.html>>

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.