

CRYPTO-GRAM
15 febbraio 2006

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:

[I rischi legati alla perdita di dispositivi portatili](#)
[Documenti d'identità multiuso](#)
[Benjamin Franklin sulla percezione della sicurezza](#)
[La sicurezza nel giorno di San Valentino](#)
[Le ristampe di Crypto-Gram](#)
[La Dogana statunitense apre la corrispondenza internazionale](#)
[Il fallimento del programma US-VISIT](#)
[Furto d'identità nel Regno Unito](#)
[News](#)
[Passlogix mi cita erroneamente nel proprio materiale PR](#)
[Il Canile: Super Cipher P2P Messenger](#)
[Privatizzare il programma Registered Traveler](#)
[Le News di Counterpane](#)
[Problemi di sicurezza con i sistemi ad accesso controllato](#)
[Alcune vignette sul tema della sicurezza](#)
[Contrastare "Trusting Trust"](#)
[La sicurezza nella "nuvola"](#)
[Commenti dei lettori](#)

** **

I rischi legati alla perdita di dispositivi portatili

Alcuni anni fa dimenticai il mio computer portatile su un treno che da Washington era diretto a New York. Sostituire il portatile mi costò molto denaro, ma a quel tempo ero più preoccupato dei miei dati.

Naturalmente avevo un buon backup di tutto, ma una copia di tutte le mie email, dei file dei clienti, degli scritti personali e dei manoscritti dei miei libri si trovava altrove, da qualche parte. Probabilmente il nuovo proprietario ha subito cancellato l'hard disk, ma forse la mia vita professionale e privata potrebbe essere finita in luoghi indesiderati.

Questo problema è andato aggravandosi. Oggi i vari dispositivi digitali sono sempre più piccoli e allo stesso tempo sono in grado di contenere una quantità sempre maggiore di informazioni sensibili.

Il portatile è il mio computer principale. Può facilmente contenere tutti i messaggi email da me inviati e ricevuti negli ultimi 12 anni, un'enorme quantità di documenti di lavoro, e tutte le mie cose.

Possiedo diverse chiavette USB, fra cui un minidrive da 2 GB che serve da backup principale. Nel drive che mi porto appresso è contenuta una copia completa degli ultimi 12 mesi della mia vita; si tratta di un dispositivo talmente facile da smarrire che molte persone che conoscono ne comprano parecchi alla volta.

Il mio telefono cellulare è un Treo. Non solo contiene i numeri di telefono che chiamo più frequentemente, ma anche l'intera rubrica indirizzi (insieme a eventuali note personali che ho aggiunto), la mia agenda degli ultimi sei anni, centinaia di email, tutti i miei messaggi SMS, e un registro di tutte le chiamate da me effettuate e ricevute. O almeno così sarebbe se non avessi preso particolari precauzioni per cancellare tali informazioni di tanto in tanto.

Un mio amico ha l'abitudine di scordarsi il suo iPod sugli aerei; finora ne ha perduti tre. L'iPod che ha smarrito più di recente conteneva non solo la sua intera libreria musicale, ma anche la sua agenda e la sua rubrica indirizzi. E la stampa riporta spesso notizie di computer portatili smarriti e/o rubati contenenti documenti aziendali riservati o informazioni personali di centinaia di migliaia di individui.

Potrei andare avanti per ore.

Il punto è che oggi è incredibilmente facile perdere un'enorme quantità di dati. Vent'anni fa, una persona avrebbe potuto penetrare nel mio ufficio e copiare ogni singolo file sui miei clienti, ogni documento di corrispondenza, tutto quel che riguarda la mia vita professionale. Adesso tutto quel che gli basta fare è rubarmi il portatile, o il mio minidrive di backup, o i miei DVD di backup. Inoltre potrebbe comunque penetrare nel mio ufficio e copiarsi tutte queste informazioni senza che io me ne possa accorgere in un secondo momento.

Questo problema non è destinato a risolversi molto presto.

Vi sono due possibili soluzioni sensate. La prima è quella di proteggere i dati. Programmi di crittografia dell'hard disk come PGP Disk permettono di criptare singoli file, cartelle o intere partizioni disco. Diversi produttori commercializzano chiavette USB dotate di crittografia incorporata. Alcuni produttori di PDA stanno incominciando ad aggiungere la protezione con password ai loro dispositivi (non efficace quanto la crittografia, ma è pur sempre qualcosa), e vi sono alcuni programmi di crittografia scritti apposta per i PDA.

La seconda soluzione è quella di cancellare i dati in via remota in caso di smarrimento del dispositivo. Si tratta di un'idea ancora nuova, ma sono sicuro che prenderà piede nel mercato aziendale. Se si fornisce un Blackberry per uso aziendale a un impiegato, si deve essere in grado di cancellare la memoria del dispositivo nel caso l'impiegato lo smarrisca. E dato che il Blackberry è sempre online, è una funzionalità molto semplice da aggiungere.

Ma fino a quando queste due soluzioni non verranno largamente adottate, la cosa migliore da fare è prestare attenzione e cancellare i dati. Cancellate dal vostro Blackberry tutte le vecchie email, i messaggi SMS dal cellulare, e i vecchi dati dalle vostre rubriche indirizzi con regolarità. Cercate il registro delle chiamate sul cellulare e cancellatelo di tanto in tanto. Non immagazzinate di tutto sul vostro portatile, ma solo i file che possano davvero servirvi.

Non credo si possano rendere questi dispositivi più difficili da smarrire: si tratta di un problema umano e non tecnologico. Ma almeno possiamo fare in modo che la perdita sia solo economica e non di privacy.

Questo articolo è originariamente apparso su Wired.com:
<<http://www.wired.com/news/technology/0,70044-0.html>>

Un ufficiale dell'esercito olandese ha smarrito una memory stick contenente dettagli top secret di una missione afgana.
<http://www.expatica.com/source/site_article.asp?subchannel_id=1&story_id=27303&name=Officer+lost+USB+stick+with+details+of+Afghan+mission> oppure
<<http://tinyurl.com/ahm7f>>

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

Documenti d'identità multiuso

Non so il vostro portafoglio, ma il mio contiene una patente di guida, tre carte di credito, due bancomat, tessere frequent flier di tre diverse compagnie aeree e tessere frequent guest per tre diverse catene alberghiere, nonché le tessere socio per due club di linee aeree, una tessera della biblioteca, una tessera AAA, una tessera d'iscrizione Costco, e svariati altri documenti che attestano la mia identità.

Un qualsiasi tecnologo che osservasse questa montagna di schede mi chiederebbe, giustamente: perché tutte quelle tessere? La maggior parte di esse non è stata realizzata con l'intento di essere un documento d'identità difficile da falsificare: si

tratta semplicemente di modi per avere con sé numeri identificativi che non sono altro che puntatori in un database. Perché Visa si preoccupa in primo luogo di emettere carte di credito? È evidente come non sia necessaria la tessera fisica per completare una transazione, come ben sanno coloro i quali hanno acquistato dei beni via internet o per telefono. La banca potrebbe semplicemente utilizzare il codice della patente di guida come numero di conto.

Stesso dicasi per quelle tessere di fidelizzazione di linee aeree, alberghi, autonoleggi, o per quelle tessere di sconto emesse da supermercati, negozi di cancelleria per ufficio, ferramenta... praticamente da ogni genere di esercizio commerciale. Tutti potrebbero servirsi di vostri numeri di conto già esistenti, o anche più semplicemente, del vostro nome e indirizzo. Infatti, se perdete una tessera, troveranno il vostro numero di conto se fornite loro il vostro numero di telefono. Perché affrontare le spese e i problemi legati all'emissione di carte diverse?

Un sistema di autenticazione unico e centralizzato è stato per molto tempo il sogno di molti tecnologi. Chi si occupa di sicurezza informatica si ricorderà la promessa dell'infrastruttura a chiave pubblica (PKI). Tutti avrebbero avuto un singolo "certificato" digitale che sarebbe stato accettato da ogni genere di applicazioni. Non si è mai realizzato niente del genere.

E oggi le proposte di ampia portata che riguardano documenti di identità nazionali (compresa una recente proposta in Sud Africa) immaginano un mondo in cui un unico ID verrà utilizzato per ogni cosa. Non si realizzerà neanche questo.

E nemmeno si realizzerà l'ipotesi biometrica. È il prossimo, ovvio, passaggio: perché avere con sé una patente di guida? Basta il proprio volto o un'impronta digitale.

Ma la verità è che nemmeno un documento d'identità nazionale o un sistema biometrico soppianteranno mai i mazzi di schede plastificate che affollano i nostri portafogli.

Tanto per cominciare, l'unicità delle schede offre un'importante sicurezza per chi le emette. Ogni compagnia possiede norme differenti che regolano l'emissione della carta, la scadenza e la revoca, e ognuna vuole essere in grado di controllare le proprie carte. Se si perde il controllo, si perde sicurezza. Quindi i club delle linee aeree richiedono una fototessera d'identità insieme alla tessera di socio, e i commercianti vogliono vedere un documento d'identità quando si utilizza una carta di credito, ma nessuno di essi rimpiazzerà la propria carta o tessera a favore di quel documento di identità.

Un altro motivo è l'affidabilità e la regolarità di funzionamento. La vostra compagnia di carta di credito non desidera che la vostra capacità di effettuare acquisti venga inibita per esempio da un ritiro della patente di guida. La vostra compagnia aerea non vuole che il vostro account frequent flier dipenda da una particolare carta di credito. E nessuno desidera accettare la responsabilità di far dipendere la propria applicazione dall'infrastruttura altrui, o di fare in modo che la propria infrastruttura supporti le applicazioni di terzi.

Ma sicurezza e affidabilità sono solo preoccupazioni secondarie. Se fosse un vantaggio di business per le varie aziende affidarsi a tessere e carte già esistenti, troverebbero un sistema per risolvere le problematiche di sicurezza. La ragione per cui non lo fanno si può riassumere in una parola: branding.

La mia compagnia aerea vuole che io possieda una tessera con il suo logo stampato su di essa. Così come la compagnia di autonoleggio, il supermercato e tutte le altre entità con cui ho un rapporto d'affari. La compagnia di carta di credito vuole che io apra il portafoglio e che noti la sua carta: è più probabile che io utilizzi una carta di credito fisica che non una virtuale che devo ricordarmi essere collegata al mio numero di patente di guida. Ed è più probabile che io mi senta importante se possiedo una tessera vera e propria, soprattutto una tessera che mi riconosca quale frequent flier o cliente privilegiato.

Alcuni anni fa, quando le carte di credito con chip incorporato erano una novità, i produttori delle carte progettaronò un sistema multi-applicazione sicuro per queste smart card. L'idea era che un'unica carta fisica potesse essere utilizzata per qualsiasi cosa: svariati conti di carte di credito, tessere di affiliazione a linee aeree, tessere di abbonamento a trasporti pubblici, eccetera. Nessuno si affidò a questo sistema: non per ragioni di sicurezza, ma per motivi di branding. Quale logo avrebbe esposto la famigerata tessera unica? Quando i produttori pensarono a una carta che presentasse tutti i vari loghi in piccolo, uno per ogni applicazione, tutti vollero sapere: quale logo sarà il primo della fila? O quello più in alto? O a colori?

Le varie aziende vi forniscono le loro proprie carte e tessere in parte perché desiderano avere il completo controllo delle norme dettate dal loro sistema, ma soprattutto perché vogliono che abbiate con voi un piccolo oggetto pubblicitario. Una Carta Oro di American Express dovrebbe farvi sentire potenti e invidiati dagli altri. E American Express vuole che la mostriate in giro.

Ecco perché continuiamo a ritrovarci dozzine di tessere nel portafoglio. E quei paesi che possiedono documenti di identità nazionali forniscono ai propri cittadini un'ennesima carta da portarsi appresso, e non un qualcosa che sostituisca qualcos'altro.

Questo articolo è originariamente apparso su Wired.com:
<<http://www.wired.com/news/technology/0,70167-0.html>>

** *** *****

Benjamin Franklin sulla percezione della sicurezza

Il 17 gennaio è stato il 300esimo anniversario della nascita di Benjamin Franklin. Oltre alle sue varie invenzioni e scoperte, Franklin trovò il modo di proteggere gli edifici dai fulmini, sistemando una o più barre appuntite sulla sommità di un edificio e fornendo un tracciato di conduzione verso terra all'esterno dell'edificio stesso. Molta

gente provò questo sistema e funzionò. Franklin divenne una celebrità, non solo fra gli "elettricisti", ma per il grande pubblico.

Un articolo nel numero di gennaio di "Physics Today" contiene un'eccellente citazione di Franklin del 1769, che parla dei parafulmini e della realtà delle cose contrapposta alla percezione della sicurezza:

"Coloro che calcolano i rischi troveranno forse che non più di una morte (o la distruzione di una casa) su centomila può avvenire per quella causa, e che perciò non varrebbe molto la pena spendere denaro per proteggerci da essa. Ma in ogni paese vi sono situazioni particolari per cui alcuni edifici sono più esposti di altri a tali eventualità, e che vi sono persone talmente ossessionate dal timore di tali possibilità da sentirsi minacciate ogni volta che odono il più insignificante dei tuoni; pertanto può essere buona cosa diffondere e chiarire il più possibile questo piccolo nuovo strumento, poiché il suo vantaggio non è limitato al renderci tutti più sicuri, ma ci rende in parte anche più tranquilli. E anche se quel fulmine da cui ci protegge potrà capitare forse una sola volta nella nostra vita, avrà fugato i nostri timori e le nostre angosce almeno cento volte, e questa seconda occorrenza può contribuire molto di più alla felicità degli uomini che non la prima".

<<http://www.physicstoday.org/vol-59/iss-1/p42.html>>

** *** *****

La sicurezza nel giorno di San Valentino

Venerdì scorso il Wall Street Journal presentava un articolo su come il giorno di San Valentino sia il giorno in cui i coniugi infedeli commettono imprudenze e passi falsi:

"Il giorno di San Valentino è in assoluto l'intervallo di 24 ore più proficuo per i fioristi, un grande evento per le aziende produttrici di biglietti d'auguri e una manna per chi produce dolcetti. Ma è anche un giorno di grande crisi per chiunque abbia un'altra relazione in corso. Dopotutto, San Valentino è la ricorrenza in cui ci si aspetta che tutti facciano qualcosa di romantico per il proprio coniuge o amante. E per chi ha entrambi è un grosso problema".

Pertanto, ovviamente, gli investigatori privati fanno gli straordinari.

"Se c'è qualcosa in ballo, accadrà in quel giorno", sostiene Irene Smith, la quale afferma che per la sua agenzia investigativa Discreet Investigations a Golden, nel Colorado, gli affari il giorno di San Valentino come minimo raddoppiano, fino ad arrivare a 12 casi in certi anni".

Secondo l'articolo, pagare un investigatore privato è costoso, circa 100 dollari l'ora, e può non valerne la pena.

Nell'articolo vengono poi suggeriti alcuni strumenti di sorveglianza da utilizzare in ambito domestico: un sistema di tracciamento GPS in tempo reale che è possibile

nascondere nell'auto del coniuge, un kit di rilevamento prove casalingo da usarsi per analizzare macchie su "vestiti, sedili dell'auto o in altri luoghi", software per spiare le connessioni Internet, un registratore telefonico, e una pratica minicamera da appuntare all'occhiello della giacca.

Ma anche tutta questa attrezzatura potrebbe essere eccessiva.

"Ruth Houston, autrice di un libro intitolato 'Is He Cheating on You? -- 829 Telltale Signs' [Lui vi sta ingannando? 829 indizi rivelatori], in generale sconsiglia di spendere denaro in investigatori privati perché i vari segnali sono molto facili da captare. (Indizio n. 3 della categoria 'Regali': lui cerca di convincervi di aver comprato cioccolatini molto cari per sé)".

Mi auguro che sia inutile ricordare che anche i coniugi infedeli dovrebbero leggersi quel libro e scoprire quali sono gli 829 indizi rivelatori che dovrebbero evitare di produrre.

L'articolo presenta parecchie storie personali molto interessanti, e avverte che "pianificare un 'viaggio d'affari' che va a cadere proprio nel giorno di San Valentino è il classico errore che un coniuge infedele commette".

Ora mi domando perché la RSA Conference viene tenuta proprio il giorno di San Valentino...

L'articolo del Wall Street Journal (purtroppo è disponibile solo per i sottoscrittori paganti):

<<http://online.wsj.com/article/SB113953440437870240.html>>

Sistema di tracciamento GPS in tempo reale:

<<http://spygear4u.com/>>

Lo "Home Evidence Collection Kit" (Kit di rilevamento prove casalingo):

<<http://trutestinc.com/>>

Software per spiare le connessioni Internet:

<<http://e-spy-software.com/>>

Registratore telefonico:

<<http://uspystore.com/>>

Minicamera da appuntare all'occhiello della giacca:

<<http://pimall.com/nais/buttoncamera.html>>

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

Le ristampe di Crypto-Gram

Crypto-Gram è attualmente al suo nono 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-back.html>>. Quella che segue è una selezione di articoli apparsi in questo mese gli anni scorsi.

Il programma Secure Flight di TSA:

<<http://www.schneier.com/crypto-gram-0502.html#1>>

<<http://www.cryptogram.it/cryptogramPdf/Febraio2005.pdf>> (versione italiana)

La maledizione della "Domanda Segreta":

<<http://www.schneier.com/crypto-gram-0502.html#9>>

<<http://www.cryptogram.it/cryptogramPdf/Febraio2005.pdf>> (versione italiana)

Autenticazione e relativa scadenza:

<<http://www.schneier.com/crypto-gram-0502.html#10>>

<<http://www.cryptogram.it/cryptogramPdf/Febraio2005.pdf>> (versione italiana)

Verso una sorveglianza totale

<<http://www.schneier.com/crypto-gram-0402.html#1>>

<<http://www.cryptogram.it/febraio04.htm#a1>> (versione italiana)

La politicizzazione della Sicurezza

<<http://www.schneier.com/crypto-gram-0402.html#2>>

<<http://www.cryptogram.it/febraio04.htm#a2>> (versione italiana)

Identificazione e Sicurezza

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

<<http://www.cryptogram.it/febraio04.htm#a6>> (versione italiana)

L'economia dello Spam

<<http://www.schneier.com/crypto-gram-0402.html#9>>

<<http://www.cryptogram.it/febraio04.htm#a9>> (versione italiana)

L'esercito e la Guerra Cibernetica:

<<http://www.schneier.com/crypto-gram-0301.html#1>>

<<http://www.cryptogram.it/gennaio03.htm#a1>> (versione italiana)

Il metodo di autenticazione RMAC

<<http://www.schneier.com/crypto-gram-0301.html#7>>

<<http://www.cryptogram.it/gennaio03.htm#a7>> (versione italiana)

Microsoft e il "trustworthy computing":

<<http://www.schneier.com./crypto-gram-0202.html#1>>

<<http://www.cryptogram.it/febraio02.htm#a1>> (versione italiana)

Considerazioni su Microsoft:

<<http://www.schneier.com/crypto-gram-0202.html#2>>

<<http://www.cryptogram.it/febraio02.htm#a2>> (versione italiana)

Protezione anti-copia incorporata negli hard disk:
<<http://www.schneier.com/crypto-gram-0102.html#1>>

Un attacco semantico sugli URL:
<<http://www.schneier.com/crypto-gram-0102.html#7>>

L'idiozia dei filtri e-mail:
<<http://www.schneier.com/crypto-gram-0102.html#8>>

Gli air gaps:
<<http://www.schneier.com/crypto-gram-0102.html#9>>

Il voto in Internet di contro all'e-commerce su vasta scala:
<<http://www.schneier.com/crypto-gram-0102.html#10>>

Attacchi di tipo denial-of-service distribuiti:
<<http://www.schneier.com/crypto-gram-0002.html#ddos>>

Riconoscere le prese in giro in ambito crittografico:
<<http://www.schneier.com/crypto-gram-9902.html#snakeoil>>

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

La Dogana statunitense apre la corrispondenza internazionale

La stampa ha riportato la notizia secondo cui la Dogana statunitense sta aprendo la corrispondenza internazionale in arrivo negli Stati Uniti, senza un mandato.

Purtroppo questo è legale.

Il Congresso ha passato una legge sul commercio nel 2002 (107 H.R. 3009), che estende le competenze della Dogana in merito all'apertura di corrispondenza internazionale. Ecco l'inizio della sezione 344:

"(1) In generale. – Allo scopo di assicurare la conformità alle leggi doganali degli Stati Uniti e ad altre leggi imposte dal Servizio Doganale, incluse le disposizioni di legge descritte al paragrafo (2), un funzionario doganale ha facoltà, secondo le disposizioni della presente sezione, di fermare e perquisire ai confini di stato, e senza un mandato di perquisizione, la corrispondenza originata all'interno del paese e diretta all'estero mediante il Servizio Postale Statunitense (United States Postal Service) e corrispondenza estera in transito negli Stati Uniti che sia importata o esportata dal Servizio Postale Statunitense".

Se ben ricordo, l'ACLU è stata in grado di attenuare l'emendamento, e questo linguaggio è migliore di quanto voluto in origine dal governo.

La posta prioritaria nazionale rimane privata: la polizia necessita di un mandato per aprirla. Ma vi è uno standard più basso per quanto riguarda la cosiddetta Media Mail (per inviare libri, supporti informatici, ecc., più lenta ed economica della posta prioritaria) e uno standard più basso per la cosiddetta "mail cover", ovvero la pratica di raccogliere indirizzi scritti sulle buste.

<<http://www.msnbc.msn.com/id/10740935/>>

107 H.R. 3009:

<<http://thomas.loc.gov/cgi-bin/bdquery/z?d107:h.r.3009:>>

** *** *****

Il fallimento del programma US-VISIT

US-VISIT è il programma per prendere le impronte digitali e controllare i visitatori stranieri che entrano negli Stati Uniti. Un recente articolo parla di come viene messo in opera il programma, ma è l'ultimo paragrafo ad essere il più interessante:

"Dal gennaio 2004, US-VISIT ha trattato più di 44 milioni di visitatori. Ha scoperto e arrestato circa 1000 persone per violazioni penali o legate all'immigrazione, secondo un comunicato stampa del Dipartimento per la Sicurezza Nazionale".

Scrissi in merito a US-VISIT nel 2004, e all'epoca dissi che era un programma troppo costoso e che si trattava di un pessimo compromesso. Il costo della "fase successiva" era stimato a 15 miliardi di dollari, ma sono sicuro che il costo totale è ben più alto.

Ma prendiamo quella cifra, 15 miliardi di dollari. Un migliaio di criminali, la maggior parte dei quali tutt'altro che minacciosi, catturati grazie a US-VISIT. Facendo i conti, sono 15 milioni di dollari per criminale.

Sicuramente esiste un sistema molto più efficace economicamente per catturare i criminali.

<<http://fcw.com/article91831-12-30-05-Web>>

Il mio precedente articolo sul tema:

<<http://www.schneier.com/essay-072.html>>

** *** *****

Furto d'identità nel Regno Unito

Di recente nel Regno Unito è stata commessa una grave frode legata al credito d'imposta. Esiste un sistema di credito d'imposta che permette ai contribuenti di ottenere un rimborso per alcune tasse nel caso rientrino in certi parametri. Da un

punto di vista politico, si è trattato di un obiettivo importante per il Partito Laburista. Perciò l'Inland Revenue (ossia il fisco -- corrisponde allo IRS statunitense) ha facilitato il più possibile la procedura di richiesta di tale rimborso. Uno dei modi forniti al contribuente è stato quello di sfruttare un portale Web.

Purtroppo, gli unici dati necessari per effettuare la richiesta erano il numero di previdenza sociale (National Insurance number, corrispondente al Social Security number americano) e il cognome da nubile della madre. Il rimborso veniva poi bonificato direttamente al numero di conto corrente bancario specificato nel modulo di richiesta. Chiunque abbia un minimo di conoscenze di sicurezza può immaginare quel che è accaduto. Si stima che siano stati sottratti 15 milioni di sterline da parte di organizzazioni criminali.

La stampa ha trattato questa vicenda nei termini di un furto di identità, dicendo di come i criminali abbiano fatto man bassa di numeri di previdenza sociale, e così via. Non si è detto molto su come abbia fallito lo schema di autenticazione. Il sistema cercava di autenticare la persona utilizzando informazioni semi-segrete come il numero di previdenza sociale e il cognome da nubile della madre. Invece il sistema avrebbe dovuto provare ad autenticare la transazione. Anche un semplice passaggio di verifica – il nome del conto corrisponde al nome della persona che dovrebbe ricevere il rimborso? – sarebbe stato sufficiente a prevenire questo tipo di frode.

<<http://news.bbc.co.uk/1/hi/business/4617108.stm>>

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

News

Un problema delle telecamere è che non è possibile evitare gli abusi da parte di chi osserva. Questa è la storia di due operatori di telecamere a circuito chiuso arrestati e detenuti per aver spiato una donna nuda in casa propria.

<<http://news.bbc.co.uk/1/hi/england/merseyside/4609746.stm>>

<http://www.theregister.co.uk/2006/01/13/cctv_men_jailed/>

Il Dipartimento per la Sicurezza Nazionale sta finanziando la sicurezza di prodotti open source, fra cui Linux, Apache, MySQL, FreeBSD, Mozilla e Sendmail. Ritengo che sia un utilizzo eccellente dei fondi pubblici. Uno dei limiti dello sviluppo open source è la difficoltà di finanziare strumenti come Coverity. E questo genere di iniziativa migliora la sicurezza di molte organizzazioni differenti contro una grande quantità di minacce. E aumenta la competizione con Microsoft, che sarà costretta a migliorare il proprio sistema operativo. Vittoria per tutti.

<<http://www.eweek.com/article2/0,1895,1909946,00.asp>>

Tutta la faccenda delle intercettazioni illegali da parte della NSA si è risolta in una serie di vicoli ciechi, e questo non dovrebbe sorprendere. Non è possibile ottenere altro che falsi allarmi quando si istituisce un programma di sorveglianza all'ingrosso affidandolo ai computer; l'occorrenza di trame terroristiche vere e proprie è

semplicemente troppo rara perché accada qualcos'altro. La buona sicurezza ha persone al comando e la tecnologia come strumento, non il contrario.

<<http://www.nytimes.com/2006/01/17/politics/17spy.html>>

Leggendo l'articolo qui sopra si ha l'impressione di una lotta fra bande (NSA da una parte, FBI dall'altra) per il controllo del territorio, ma gli aspetti "da partita di baseball" interna sono interessanti.

<<http://www.wired.com/news/columns/0,70035-0.html>>

Articolo interessante sui terroristi dinamitardi suicidi. La conclusione: le libertà civili aumentano la sicurezza.

<<http://www.sciam.com/article.cfm?chanID=sa006&articleID=0006A854-E67F-13A1-A67F83414B7F0104&pageNumber=2&catID=2>>

oppure <<http://tinyurl.com/ack8p>>

Grande storia di contraffazione, che illustra come i criminali si adattino alle contromisure di sicurezza. Come precauzione di sicurezza, i commercianti utilizzano una penna chimica che può rilevare se una banconota è fasulla. Ma questo non è esattamente ciò che fa la penna: essa in realtà verifica soltanto la bontà della carta. Per cui i criminali prendono banconote di piccolo taglio, le cancellano, e le modificano in banconote da grosso taglio.

<<http://news.tbo.com/news/metro/MGB60FN8IIE.html>>

Lo scorso mese è stato il 20esimo anniversario del primo virus per PC: Brain.

<<http://www.f-secure.com/v-descs/brain.shtml>>

<<http://www.f-secure.com/weblog/archives/archive-012006.html#00000784>>

oppure <<http://tinyurl.com/7wnl4>>

Alcuni dettagli su come funzionano i cani anti-bomba:

<<http://www.slate.com/id/2134394/>>

Anonym.OS è un sistema operativo anonimo. Si basa su CD, progettato in modo da non toccare mai l'hard disk. È possibile utilizzarlo su un computer pubblico e navigare in Internet in modo anonimo. Ritengo importante questo tipo di strumenti, e mi fa piacere vederne lo sviluppo.

<<http://www.wired.com/news/technology/0,70017-0.html>>

<<http://theory.kaos.to/projects.html>>

<<http://yro.slashdot.org/article.pl?sid=06/01/16/2142208>>

Il Dipartimento della Difesa degli Stati Uniti intende sviluppare una macchina della verità che possa essere impiegata di nascosto (sicuro, chi non ne vorrebbe una?).

<<http://www.newscientist.com/article.ns?id=mg18925335.800>>

In questo articolo sulle tessere RFID vi è un paragrafo che sostiene che il chip può essere letto "a distanza di svariati metri ai posti di frontiera". Credevo che il governo stesse ancora sostenendo che i chip potessero essere letti solamente ad alcuni centimetri di distanza.

<http://www.latimes.com/news/nationworld/nation/la-na-border18jan18_0,1125973.story>

oppure <<http://tinyurl.com/ch8d5>>

Trovato il 43esimo numero primo di Mersenne: $2^{30.402.457} - 1$, grazie a una colossale ricerca parallela. È lungo 9.152.052 cifre decimali.

<<http://www.mersenne.org/prime.htm>>

Un articolo su come in Francia venga utilizzato lo spionaggio interno come strumento antiterrorismo. Mi fa piacere leggere come in tutta la procedura sia intimamente coinvolto anche un giudice.

<http://www.foreignpolicy.com/story/cms.php?story_id=3353>

Come sopravvivere a una rivolta dei robot:

<<http://www.livejournal.com/users/bohunk/1561641.html>>

<http://www.schneier.com/blog/archives/2006/01/how_to_survive.html>

Se avete un momento, rispondete a questo questionario sulla divulgazione delle vulnerabilità. I ricercatori stanno cercando di capire come si possano bilanciare segretezza e apertura nell'analisi e negli avvisi relativi alle vulnerabilità di sicurezza.

<<http://www.infowarrior.org/survey.html>>

Affascinanti informazioni sullo spionaggio in Nuova Zelanda:

<<http://www.stuff.co.nz/stuff/print/0,1478,3540743a6005,00.html>>

EPIC è in possesso di documenti che mostrano come contratti "no-bid" (ossia senza gare d'appalto) per lavorare sugli standard dei sistemi di voto vadano ai rivenditori di quelle macchine.

<http://www.epic.org/foia_notes/note11.html>

Una triste vicenda legata alla no-fly list statunitense. La persona in questione stava viaggiando dal Canada al Messico. Il suo aereo non è atterrato negli Stati Uniti, li ha solamente sorvolati. Un altro errore di persona, naturalmente.

<http://www.thestar.com/NASApp/cs/ContentServer?pagename=thestar/Layout/Article_Type1&c=Article&cid=1136589011746&call_pageid=968332188854&col=96835060724> oppure <<http://tinyurl.com/dsxnn>>

E questa è la storia di un bambino di quattro anni il cui nome è nella watch list:

<<http://abclocal.go.com/ktrk/story?section=local&id=3771743>>

Il Domestic Technology Transfer Program (DTTP) della NSA:

<<http://www.nsa.gov/techtrans/index.cfm>>

Si dia anche un'occhiata ai loro "44 Technology Profile Fact Sheets":

<<http://www.nsa.gov/techtrans/techt00002.cfm>>

Ricevo molte email, a volte sono email bizzarre. Di tanto in tanto ricevo una email da qualcuno che ha bisogno della risoluzione di un crittogramma originale scritto a mano. Questo è del 2004 e riguarda un duplice omicidio e un suicidio. Il crittogramma è stato lasciato dall'omicida, ed è sul mio blog. Date un'occhiata, alla nota e ai commenti, se siete interessati a tentare di risolvere il mistero. Ma abbiate rispetto dei parenti e degli amici delle vittime: anch'essi stanno seguendo i progressi sul blog.

<http://www.schneier.com/blog/archives/2006/01/handwritten_rea.html>

Il documento del SANS intitolato "The 2005 Information Security Salary and Career Advancement Survey" [Indagine sulle retribuzioni e gli avanzamenti di carriera nell'ambito dell'Information Security nel 2005] è una lettura interessante.

<<http://www.sans.org/salary2005>>

Scoperto un dead drop wireless ad alta tecnologia in Russia. Affascinante.

<<http://en.rian.ru/russia/20060130/43250990.html>>

<<http://news.bbc.co.uk/2/hi/europe/4639758.stm>>

<http://www.schneier.com/blog/archives/2006/01/wireless_dead_d.html>

Mi viene in mente una tecnica dead drop utilizzata, se non erro, dai terroristi dell'11 settembre. Si servirono di account Hotmail (o di un altro servizio email anonimo), ma invece di inviarsi messaggi email fra loro, uno salvava il messaggio come bozza, e il destinatario lo avrebbe letto autenticandosi nel medesimo account. Un'idea davvero astuta.

Un paio di hacker olandesi hanno craccato il passaporto biometrico del loro paese. Due fatti saltano all'occhio. Primo, il chip RFID nel passaporto può essere letto da dieci metri di distanza. Secondo, tanta prevedibilità nella chiave crittografica (troppo, troppo approssimativa) rende l'attacco brute force assai più facile. Ma i riferimenti sono della scorsa estate. Perché la notizia viene riportata solo ora?

<http://www.theregister.com/2006/01/30/dutch_biometric_passport_crack/>

Un bug nel servizio censurato di Google per la Cina:

<<http://www.crypticide.com/dropsafe/articles/security/post20060129233439.html>>

oppure <<http://tinyurl.com/792x9>>

E ora funziona, utilizzando "tiananmen" come termine da ricercare:

<<http://www.computerbytesman.com/google/imagesearch.htm?tiananmen>>

La NSA su come redigere documenti per la pubblicazione (MS Word e PDF):

<<http://www.fas.org/sgp/othergov/dod/nsa-redact.pdf>>

Qui vi sono altre Guide di Configurazioni di Sicurezza:

<<http://www.nsa.gov/snac>>

Interessante articolo riguardante un individuo incarcerato per aver realizzato un botnet a scopo di lucro:

<<http://www.breitbart.com/news/2006/01/23/D8FALFU05.html>>

Una prigionia olandese ad alta tecnologia dove "i detenuti indossano bracciali elettronici che tracciano ogni loro movimento e le guardie controllano le celle utilizzando software di riconoscimento emotivo". Software di riconoscimento emotivo? Wow. Si ricordi che le nuove tecnologie di sorveglianza vengono prima impiegate su comunità dai diritti limitati: detenuti, bambini, personale militare, e i malati di mente.

<<http://www.cnn.com/2006/TECH/01/19/high.tech.prisons.ap>>

Interessante libro bianco dall'ACLU: "Eavesdropping 101: What Can The NSA Do?" [ABC dell'intercettazione: che cosa può fare la NSA?]

<<http://www.aclu.org/safefree/nsaspying/23989res20060131.html>>

<<http://www.aclu.org/safefree/nsaspying/nsamap013006.html>>

<<http://www.politechbot.com/2006/01/31/barry-steinhardt-on>>

Degli ignoti hanno intercettato i telefoni cellulari di circa 100 politici greci e i relativi uffici, fra cui l'ambasciata americana di Atene e l'ufficio del primo ministro greco. I dettagli sono sommersi, ma pare che sia stato scoperto del codice malevolo dai tecnici Ericsson nel software di Vodafone. Il codice si metteva in ascolto nella modalità di chiamata in conferenza. Impostava una chiamata in conferenza con altri 14 cellulari prepagati, mediante i quali venivano registrate le chiamate.

<<http://betabug.ch/blogs/ch-athens/288>>

<http://seattlepi.nwsource.com/national/1103AP_Greece_Phone_Surveillance.html>

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

Ulteriori informazioni in greco:

<<http://www.in.gr/news/article.asp?lngEntityID=681341&lngDtrID=244>>

Un interessante studio di ricerca a cura di Shishir Nagaraja e Ross Anderson, "The Topology of Covert Conflict" [La topologia del conflitto nascosto]. Collegamenti allo stato di guerra, al terrorismo e alle reti di condivisione peer-to-peer:

<<http://www.cl.cam.ac.uk/TechReports/UCAM-CL-TR-637.html>>

Lo scorso anno ho parlato di un articolo scritto da Daniel J. Solove e Chris Hoofnagle intitolato "A Model Regime of Privacy Protection" [Un regime moderno di protezione della privacy]. Lo scritto è stato revisionato alcune volte grazie ai commenti pervenuti (alcuni da lettori del mio blog e di Crypto-Gram) e pubblicato.

<http://papers.ssrn.com/sol3/papers.cfm?abstract_id=881294>

Le possibilità che tutto questo diventi una legge sono, purtroppo, tendenti a zero.

Questo club di Barcellona richiede un chip RFID incorporato per accedere allo status di VIP:

<<http://edition.cnn.com/2004/TECH/10/05/spark.bajabeach/>>

E questa azienda richiede la stessa cosa per l'accesso al centro di elaborazione dati:

<http://www.theregister.co.uk/2006/02/10/employees_chipped/>

<<http://www.securityfocus.com/brief/134>>

Un eccellente articolo di Malcolm Gladwell sul profiling e le generalizzazioni:

<http://www.newyorker.com/fact/content/articles/060206fa_fact>

Un'interessante confutazione dello schema di comunicazioni classiche teoricamente sicuro di Laszlo Kish:

<<http://terrybollinger.com/qencrypt/BollingerCritiqueOfKishPaper-2006-01-31.pdf>>

oppure <<http://tinyurl.com/as63o>>

E una risposta di Kish:

<http://www.ece.tamu.edu/~noise/research_files/Response_Bollinger.pdf>

Il mio articolo originale sull'argomento:

<http://www.schneier.com/blog/archives/2005/12/totally_secure.html>

Il riciclo di assegni è un tipo di frode. Il criminale si serve di vari solventi per cancellare i dati da un assegno firmato (il beneficiario dell'assegno, la cifra da pagare) e sostituirli con dati maggiormente vantaggiosi per il criminale: il proprio nome e una cifra più grossa. Questa pagina Web (non so nulla di queste persone, ma il livello sembra un po' amatoriale) parla di questo genere di frode e offre alcuni consigli a chi scrive assegni su quali penne e inchiostri utilizzare.

<<http://www.ckfraud.org/washing.html>>

Interessante studio sui nomi dati agli animali domestici, che cerca di risolvere i problemi di sicurezza legati alla scelta dei nomi.

<<http://www.skyhunter.com/marcs/petnames/IntroPetNames.html>>

La militarizzazione del lavoro della polizia: sempre più spesso le forze dell'ordine utilizzano armi e tattiche di tipo militare. "Peter Kraska, della Eastern Kentucky University – un esperto di militarizzazione della polizia ampiamente citato – stima che le squadre SWAT siano chiamate a intervenire 40.000 volte in un anno negli Stati Uniti; negli anni Ottanta le chiamate erano 3.000 all'anno. La maggior parte degli interventi serviva a presentare un mandato di arresto nei confronti di criminali non violenti legati al traffico di droga".

<http://www.cato.org/pub_display.php?pub_id=5439>

Un articolo davvero interessante sulle caratteristiche di sicurezza di Internet Explorer 7:

<<http://redmondmag.com/columns/article.asp?editorialid=1215>>

Il mio commento:

<http://www.schneier.com/blog/archives/2006/02/the_new_interne.html>

La TSA ha annunciato che Secure Flight, il suo programma a tutto campo per verificare i passeggeri delle linee aeree mediante watch list antiterrorismo, è stato sospeso. Ho scritto estesamente in merito a questo programma. È un colossale pasticcio in ogni suo aspetto, e non ci rende più sicuri. Ma non crediate che questa sia la fine. Sotto la Sezione 4012 dell'Intelligence Reform and Terrorism Prevention Act, il Congresso ha ordinato alla TSA di istituire un programma per effettuare lo screening di ogni passeggero nazionale, confrontandolo con la watch list. Finché il Congresso non revocherà quel mandato, questi rinvii e sospensioni sono la cosa migliore che possiamo sperare. Aspettatevi un imminente ritorno di tutto questo sotto un altro nome (e con una "fedina pulita" agli occhi dei più distratti).

<<http://msnbc.msn.com/id/11254968/>>

Il mio intervento su Secure Flight:

<http://www.schneier.com/blog/archives/2005/09/secure_flight_n_1.html>

Ho appena trovato uno studio interessante: "Windows Access Control Demystified" [Il controllo accessi di Windows chiarificato] di Sudhakar Govindavajhala e Andrew W. Appel. In pratica gli autori dimostrano che aziende come Adobe, Macromedia, ecc., presentano errori nella loro programmazione del controllo accessi che aprono falle di sicurezza in Windows XP.

<<http://www.cs.princeton.edu/~sudhakar/papers/winval.pdf>>

Ed Felten commenta ottimamente questo studio nel suo blog:

<<http://www.freedom-to-tinker.com/?p=970>>

Scordatevi lo RFID: è possibile essere tracciati a distanza di parecchie centinaia di metri usando il WiFi.

<<http://us.gizmodo.com/gadgets/wireless/wifi-tracking-008264.php>>

A proposito di WiFi, è probabile che Apple aggiunga questa funzionalità nei prossimi iPod:

<http://www.reghardware.co.uk/2006/02/08/portalplayer_wireless_ipod_chip/>

oppure <<http://tinyurl.com/74t7o>>

E non dimentichiamo che è sempre possibile essere tracciati attraverso il telefonino:
<http://news.com.com/E-tracking+through+your+cell+phone/2010-1039_3-6038468.html> oppure <<http://tinyurl.com/7gaxm>>

Gary T. Marx è un professore di sociologia al MIT, e scrive spesso di problematiche di privacy. Lo trovo molto chiaro e acuto, interessante e piacevole da leggere. Vale davvero la pena leggere questo nuovo studio: "Soft Surveillance: The Growth of Mandatory Volunteerism in Collecting Personal Information – 'Hey Buddy Can You Spare a DNA?'" [Sorveglianza leggera: la crescita del volontariato obbligatorio nella raccolta di informazioni personali - 'ehi amico, mi offri del DNA?'].

<<http://web.mit.edu/gtmarx/www/softsurveillance.html>>

È possibile leggere molti altri suoi articoli a questa pagina:

<<http://web.mit.edu/gtmarx/www/garyhome.html#Online>>

Vere e proprie tessere d'identità fasulle. O forse sono vere tessere d'identità falsificate. Questo sito Web vende documenti di identità. Non sono tessere identificative di nulla in particolare, ma hanno un aspetto ufficiale. Se vi occorre ingannare qualcuno che non abbia idea di come sia fatto un vero documento d'identità, è probabile che queste funzionino.

<<http://www.real-id.com/>>

** **

Passlogix mi cita erroneamente nel proprio materiale PR

Di recente ho ricevuto un'email con materiale informativo da un'azienda chiamata Passlogix. Parte del messaggio diceva: "La sicurezza delle password è tuttora una minaccia molto diffusa; nel 2005, guru della sicurezza quali Bruce Schneier hanno suggerito pubblicamente di scrivere le password su foglietti e post-it. Un recente sondaggio ha rilevato che il 78% degli impiegati utilizza password come forma principale di sicurezza, il 52% usa la stessa password per i loro vari account, eppure il 77% fatica a ricordarsi le proprie password".

In realtà io non ho detto questo. Io consiglio di trascrivere le proprie password su un foglietto da conservare nel portafoglio.

Non conosco questa azienda, ma non mi piace come ha travisato le mie parole.

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

Il mio consiglio:

<http://www.schneier.com/blog/archives/2005/06/write_down_your.html>

** **

Il Canile: Super Cipher P2P Messenger

Super Cipher P2P Messenger utilizza "un'impenetrabile crittografia Infinity bit Triple Layer Socket per comunicazioni completamente sicure".

<<http://www.snapfiles.com/get/supercipherp2p.html>>

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

Privatizzare il programma Registered Traveler

A metà gennaio la TSA ha annunciato i dettagli del suo programma Registered Traveler (a volte conosciuto come "Trusted Traveler"). In pratica si paga per avere un background check e ottenere un ID biometrico (un'impronta digitale) che permette di passare i controlli di sicurezza agli aeroporti più velocemente.

Ho già scritto del perché questa sia una pessima idea per la sicurezza:

"Ciò che il programma Trusted Traveler produce è creare due diversi percorsi di accesso all'interno dell'aeroporto: massima sicurezza e minima sicurezza. L'idea è che solo le brave persone entreranno nella corsia di minima sicurezza, e che i malviventi saranno costretti ad entrare nella corsia di massima sicurezza, ma raramente cose del genere funzionano così. È necessario presumere che i malviventi troveranno un modo per entrare nella corsia a minima sicurezza.

"Il programma Trusted Traveler è basato sul mito, assai pericoloso, secondo cui i terroristi corrispondono ad un certo profilo, e che si possa essere in grado di individuare i terroristi in una folla dopo aver identificato tutte le persone. Questo è semplicemente falso. Molti dei terroristi dell'11 settembre erano individui sconosciuti, e non appartenenti a nessuna watch list. Prima di far saltare il palazzo federale di Oklahoma City, Timothy McVeigh era un probò cittadino statunitense. I bombaroli suicidi palestinesi in Israele sono persone normali e non classificabili. I rapporti dell'Intelligence indicano che al Qaeda sta reclutando terroristi non arabi per le sue operazioni negli USA".

Ma ciò che la TSA sta facendo veramente è ancor più bizzarro: sta privatizzando questo sistema. Vuole che a effettuare i background check siano le compagnie che *vendono* a scopo di lucro i pass Registered Traveler. Vuole che per fare questo le compagnie utilizzino database commerciali pieni di errori. Quali incentivi hanno tali compagnie per non vendere il pass a chiunque? Chi è responsabile in caso di errori?

Credevo che la sicurezza delle linee aeree fosse una cosa importante.

<<http://www.tsa.gov/public/display?theme=40&content=090005198018c349>>

La notizia:

<<http://www.washingtonpost.com/wp-dyn/content/article/2006/01/20/AR2006012001812.html>>

oppure <<http://tinyurl.com/9axu6>>

Il mio precedente intervento:

<<http://www.schneier.com/essay-051.html>>

Questa è un'eccellente discussione dei problemi:

<<http://arstechnica.com/news.ars/post/20060125-6052.html>>

"Che c'è di peggio di avere dei ladri di identità che vi impersonano in banca? Avere dei terroristi che vi impersonano con la TSA".

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

Le News di Counterpane

Counterpane nel 2005 ha monitorato qualcosa come 100 miliardi di eventi di rete, in tutto il mondo. Questi sono i tipi di attacchi che stiamo vedendo:

<<http://www.counterpane.com/cgi-bin/attack-trends-cg.cgi>>

In occasione della RSA Conference, mia moglie ed io abbiamo scritto una guida di 110 pagine sui ristoranti della zona del centro di San Jose. È una lettura divertente anche per chi non stia cercando un ristorante a San Jose. (Lo sapevate che scrivo recensioni di ristoranti per il Minneapolis Star Tribune?). La guida ai ristoranti sarà disponibile alla conferenza, e naturalmente è possibile scaricarla da Internet, ma posso distribuire alcune centinaia di copie qui. Invierò una copia a chiunque la richieda, in cambio delle spese postali (non è per il denaro, ma mi occorre un sistema che possa garantire una copia della guida solo a chi è davvero interessato). Le tariffe: 2,50 dollari se siete negli USA, 3 dollari per il Canada e il Messico, 6 dollari per il resto del mondo. Accetto pagamenti via PayPal al mio indirizzo, schneier@counterpane.com, o assegni intestati a Bruce Schneier, Counterpane Internet Security, Inc., 1090A La Avenida, Mountain View, CA 94043. Mi spiace ma non posso accettare carte di credito direttamente.

<<http://www.schneier.com/restaurants-rsa2006.pdf>>

Lo scorso finesettimana sono intervenuto alla ACLU Washington Annual Membership Conference. Il Seattle Times ha registrato il mio discorso:

<http://seattletimes.nwsourc.com/html/localnews/2002800247_aclu12m.html>

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

<<http://www.aclu-wa.org/detail.cfm?id=391>>

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

Problemi di sicurezza con i sistemi ad accesso controllato

In un articolo sulla recente sparatoria all'ufficio postale vi era un'interessante dettaglio sulla sicurezza. "Il pass che consentiva all'aggressore di entrare nella struttura era scaduto, hanno affermato gli agenti, ma pare che la persona abbia sfruttato le sue conoscenze su come funziona la sicurezza nell'edificio per riuscire a

penetrarvi, seguendo un altro veicolo che entrava dal cancello esterno e obbligando altri impiegati ad aprire le porte di sicurezza”.

Questo è un errore sia tecnologico che procedurale. Il cancello era configurato per permettere l'ingresso a più veicoli usando l'autorizzazione di una sola persona – questo è l'errore tecnologico, e le persone sono addestrate a essere educate, tenendo la porta aperta per gli altri.

Nota 1: Esiste un mito assai comune secondo cui nella casistica degli omicidi sul luogo di lavoro il Servizio Postale Statunitense sia al primo posto (da cui l'espressione “going postal”, infuriarsi). Però senza contare questo evento, negli ultimi 20 anni vi è stato meno di un omicidio all'anno negli uffici delle Poste. Dato che il Servizio Postale Statunitense (USPS) conta più di 700.000 dipendenti, questo è un tasso molto più basso rispetto alla media dei luoghi di lavoro.

Nota 2: Secondo alcune notizie l'aggressore ha puntato la pistola a un altro dipendente per ottenere il suo badge, il che è un genere completamente diverso di errore.

<<http://www.msnbc.msn.com/id/11107022/>>

** *** *****

Alcune vignette sul tema della sicurezza

RFID:

<<http://www.ibiblio.org/Dave/Dr-Fun/df200601/df20060116.jpg>>

Sullo spam:

<<http://ars.userfriendly.org/cartoons/?id=20060131>>

Sui posti di controllo negli aeroporti:

<<http://www.ucomics.com/closetohome/2006/02/07/>>

** *** *****

Contrastare “Trusting Trust”

Nel 1974, Paul Karger e Roger Schell scoprirono un attacco devastante ai danni dei calcolatori. Ken Thompson lo descrisse nel suo classico discorso del 1984, “Reflections on Trusting Trust”. In pratica, un aggressore modifica un compilatore in modo che produca versioni malevole di alcuni programmi, SE STESSO COMPRESO. Una volta fatto questo l'attacco si perpetua in maniera sostanzialmente non rilevabile. Thompson ha dimostrato l'attacco in modo sconvolgente, modificando il compilatore di una vittima sperimentale, così da poter autenticarsi come root senza dover usare una password. La vittima non ha mai notato l'attacco, persino quando

sono stati disassemblati i binari: il compilatore aveva alterato anche il disassemblatore.

Questo attacco è stato per lungo tempo parte della tradizione della sicurezza informatica, e tutti sanno che non vi è difesa. Ed è questo a rendere così interessante un nuovo studio di David A. Wheeler. È intitolato "Countering Trusting Trust through Diverse Double-Compiling" [Contrastare Trusting Trust attraverso il Diverse Double-Compiling], e descrive una tecnica chiamata appunto Diverse Double-Compiling (DDC) che rileva questo attacco. Cito dal riassunto: "Basta ricompilare il presunto codice sorgente del compilatore due volte: una volta con un diverso compilatore (fidato), e una seconda volta utilizzando il risultato della prima compilazione. Se il risultato è identico bit per bit al binario sospetto, allora il codice sorgente rappresenta accuratamente il binario stesso. Questa tecnica è stata menzionata informalmente, ma le varie problematiche e implicazioni a essa collegate non sono state individuate o discusse in un lavoro sottoposto a peer review, né è stata data una dimostrazione pubblica. Questo studio descrive tale tecnica, ne dà giustificazione, descrive come superare difficoltà pratiche e la dimostra".

Per vedere come funziona, basta osservare l'attacco. Semplificando, l'aggressore modifica il compilatore in modo che ogni volta che un qualche codice di sicurezza preso come bersaglio (come il controllo di una password) viene compilato, il compilatore inserisce il codice backdoor dell'aggressore nell'eseguibile.

Ora, sarebbe facile aggirare il problema semplicemente ricompilando il compilatore. Dato che ciò viene comunque fatto di tanto in tanto, quando vengono riparati dei bug o quando vengono aggiunte delle funzionalità, una forma più robusta dell'attacco va ad aggiungere un passaggio: ogni volta che il compilatore viene compilato, esso emette il codice per inserire codice malevolo in vari programmi, compreso il compilatore medesimo.

In linea di massima, assumendo che il sorgente del compilatore venga aggiornato ma non completamente riscritto, questo attacco rimane invisibile.

Wheeler spiega come sconfiggere questo tipo più robusto di attacco. Supponiamo di avere due compilatori completamente indipendenti: A e T. Più specificatamente, abbiamo il codice sorgente S_A del compilatore A, e codice eseguibile E_A ed E_T. Vogliamo determinare se il binario del compilatore A, ossia E_A, contiene questo tipo di attacco.

Ecco il trucco di Wheeler:

Passo 1: Compilare S_A con E_A, producendo il nuovo eseguibile X

Passo 2: Compilare S_A con E_T, producendo il nuovo eseguibile Y

Dato che X e Y sono stati generati da due compilatori differenti, dovrebbero avere un codice binario diverso ma essere funzionalmente equivalenti. Per ora tutto bene. Adesso:

Passo 3: Compilare S_A con X, producendo il nuovo eseguibile V

Passo 4: Compilare S_A con Y, producendo il nuovo eseguibile W

Dato che X e Y sono funzionalmente equivalenti, V e W dovrebbero essere equivalenti bit per bit.

Ed è questo il modo per rilevare l'attacco. Se E_A è infettato dalla forma robusta dell'attacco, allora X e Y saranno funzionalmente differenti, e se X e Y sono funzionalmente differenti, allora V e W saranno differenti guardando i bit. Per cui tutto ciò che occorre fare è eseguire una comparazione binaria fra V e W: se sono diversi, E_A è infetto.

Ora potreste leggere tutto questo e pensare: "Dov'è il problema? Tutto ciò di cui ho bisogno per verificare se ho un compilatore fidato è... un altro compilatore fidato. Non è così all'infinito?"

Non proprio. Occorre fidarsi di un compilatore, ma non è necessario sapere prima di quale ci si deve fidare. Se si possiede il codice sorgente per il compilatore T, lo si può verificare rispetto al compilatore A. In pratica, occorre sempre avere almeno un eseguibile di compilatore di cui fidarsi. Ma non serve sapere di quale bisogna iniziare a fidarsi.

La definizione di "fiducia" è molto più vaga. Questa contromisura fallirà soltanto se A e T sono entrambi infettati nello stesso identico modo. Il secondo compilatore può essere malevolo, basta che lo sia in maniera diversa: ovvero, non può avere gli stessi trigger e payload del primo. Si possono aumentare le probabilità che trigger/payload non siano identici aumentando la diversità: utilizzando un compilatore di un'altra epoca, su una piattaforma diversa, senza un'eredità comune, o trasformando il codice, e così via.

Inoltre, l'UNICA cosa che il Compilatore B deve fare è compilare il compilatore-da-verificare. Può essere tremendamente lento, produrre codice tremendamente lento, o funzionare soltanto su una macchina che non viene più prodotta da dieci anni. Si potrebbe realizzare un compilatore solo ed esclusivamente per svolgere questo compito. Se siete davvero preoccupati della "regressione infinita", potete scrivervi da soli il Compilatore B per un calcolatore che avete costruito voi stessi. Dato che il Compilatore B deve solo ricompilare il vostro "vero" compilatore di tanto in tanto, potete imporre moltissime restrizioni che di solito non accettereste in un compilatore di produzione. Sarebbe possibile controllare periodicamente l'integrità del Compilatore B mediante un qualsiasi altro compilatore.

Ora, questa tecnica rileva soltanto quando il binario non coincide con il sorgente, per cui qualcuno dovrà sempre esaminare il codice sorgente del compilatore. Ma così si deve solo esaminare il codice sorgente (un compito molto più facile), e non il binario.

È interessante: l'attacco "Trusting Trust" è diventato in realtà molto più facile col tempo, perché i compilatori sono diventati sempre più complessi, fornendo agli aggressori molti più punti dove nascondere i loro attacchi. Ecco come è possibile utilizzare un compilatore più semplice (di cui ci si può maggiormente fidare) per sorvegliare un altro compilatore più complesso e sofisticato.

Lo studio di Wheeler e il sito Web:

<<http://www.acsa-admin.org/2005/abstracts/47.html>>

<<http://www.dwheeler.com/trusting-trust>>

“Reflections on Trusting Trust”:

<<http://www.acm.org/classics/sep95/>>

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

La sicurezza nella “nuvola”

Una delle filosofie di base della sicurezza è la difesa in profondità: sistemi che si sovrappongono progettati per garantire sicurezza anche nel caso uno di essi fallisca. Un esempio è dato da un firewall usato congiuntamente a un sistema antintrusione (IDS). La difesa in profondità offre sicurezza, perché non vi è nessun punto debole e presumibilmente nessun vettore per eventuali attacchi.

È per questa ragione che la scelta fra implementare la sicurezza di rete nel mezzo della rete (nella “nuvola”) o alle estremità è una falsa dicotomia. Non esiste un unico sistema di sicurezza valido per tutti, ed è preferibile scegliere di implementare la sicurezza di rete in entrambi i punti.

Questo genere di sicurezza stratificata è esattamente ciò che si sta sviluppando adesso. Tradizionalmente la sicurezza veniva implementata alle estremità, perché erano quelli che l'utente controllava. Un'organizzazione non aveva altra scelta se non inserire firewall, IDS e software antivirus all'interno della rete. Oggi, con il crescere dei servizi di sicurezza gestita e altri servizi di rete in outsourcing, è possibile aggiungere sicurezza all'interno della “nuvola”.

Io sono completamente a favore della sicurezza nella “nuvola” della rete. Se oggi potessimo costruire una nuova Internet da zero, potremmo incorporare moltissime funzionalità di sicurezza nella “nuvola”. Ma anche questo non potrebbe sostituire la sicurezza alle estremità. La difesa in profondità insiste su ogni singolo punto debole, la sicurezza nella “nuvola” è solo una parte di un approccio stratificato.

Per esempio, si considerino i vari servizi network-based di filtraggio email disponibili. Svolgono un lavoro egregio nel filtrare spam e virus, ma sarebbe una follia considerarli un sostituto del software antivirus sulla macchina desktop. Molte email sono soltanto interne, e non entrano mai nella “nuvola”. Ancor peggio, un aggressore potrebbe aprire un gateway di messaggi all'interno dell'infrastruttura aziendale. Le organizzazioni più intelligenti realizzano una difesa in profondità: filtraggio email all'interno della “nuvola” più software antivirus sulle macchine desktop.

Lo stesso ragionamento si applica ai firewall network-based e ai sistemi di Intrusion Prevention (IPS). Si potrebbe migliorare di gran lunga la sicurezza se i maggiori carrier implementassero soluzioni basate sulla “nuvola”, ma non potrebbero sostituire in tutto e per tutto i classici firewall, IDS e IPS.

Questa non dovrebbe essere mai una decisione obbligatoria fra due alternative. Counterpane, per esempio, offre servizi basati sulla "nuvola" e servizi di rete e desktop più tradizionali. Il vero tocco da maestro è far funzionare insieme le varie soluzioni.

La sicurezza riguarda la tecnologia, le persone e i processi. Non importa dove siano collocati i vostri sistemi di sicurezza, non potranno funzionare se non vi sono degli esseri umani esperti a prestare attenzione. Il monitoraggio e la risposta in tempo reale sono la cosa più importante. Dove collocare l'attrezzatura è secondario.

La sicurezza è sempre un compromesso. I budget sono limitati e le considerazioni economiche regolarmente vincono sulle decisioni di sicurezza. I servizi e i prodotti di sicurezza tradizionali sono incentrati sulla rete interna, perché è quello il bersaglio di un attacco. Anche la conformità si concentra su questo, per lo stesso motivo. La sicurezza nella "nuvola" della rete è un'ottima aggiunta, ma non può rimpiazzare una sicurezza di rete e desktop più tradizionale.

Questo articolo è stato pubblicato in un "faccia a faccia" in "Network World":
<<http://www.networkworld.com/columnists/2006/021306faceoffno.html>>

Il punto di vista opposto è qui:
<<http://www.networkworld.com/columnists/2006/021306faceoffyes.html>>

** *** *****

Commenti dei lettori

Su questi argomenti vi sono centinaia di commenti nel mio blog, molti davvero interessanti. Cercate la vicenda sulla quale intendete dare la vostra opinione, e unitevi al dibattito.

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

** *** *****

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) 2006 by Bruce Schneier.