

CRYPTO-GRAM
15 aprile 2004

Scritta da Bruce Schneier
Fondatore e CTO di Counterpane Internet Security, Inc.

Edizione italiana curata da Communication Valley SpA

E-mail: schneier@counterpane.com
Web: < <http://www.schneier.com> > oppure < <http://www.counterpane.com> >

CRYPTO-GRAM è una newsletter mensile gratuita che offre riassunti, analisi, approfondimenti, e commenti sulla sicurezza (informatica e in generale) e sulla crittografia.

Crypto- Gram in versione originale è anche consultabile in formato RSS:
< <http://www.schneier.com/crypto-gram-rss.xml> >

** **

In questo numero:

- Documenti d'identità nazionali
- Serrature autorizzate dalla TSA
- Le ristampe di Crypto- Gram
- Vincere illegalmente alle elezioni
- Le News di Counterpane
- Note di sicurezza da ogni dove: il "Man-in-the-Middle Attack"
- BeepCard
- Falla di sicurezza nel protocollo Bluetooth
- News
- Le guerre dei virus
- Commenti dei lettori

** **

Documenti d'identità nazionali

In qualità di tecnologo della sicurezza, mi capita regolarmente di incontrare persone che sostengono che gli Stati Uniti dovrebbero adottare un documento d'identità a livello nazionale. "Un sistema del genere come potrebbe non renderci più sicuri?", chiedono.

Quando un tale suggerimento proviene da una persona civile e profonda come Nicholas Kristof del New York Times, spesso il tono diventa ambivalente e carico di rimpianto: sì, certo, quel documento rappresenterebbe solo una lieve invasione della nostra privacy e senza dubbio andrebbe ad aggiungersi al già lungo elenco di inconvenienti e ritardi che incontriamo quotidianamente, ma viviamo in tempi pericolosi, in un nuovo mondo...

Tutto questo suona davvero ragionevole, ma c'è molto da ridire in merito a un simile atteggiamento.

Le potenziali usurpazioni della privacy di un sistema di carte d'identità nazionali sono tutt'altro che lievi. I ritardi e gli inconvenienti provocati da un continuo controllo di questi documenti potrebbero tranquillamente sfociare in un perenne ingorgo burocratico all'interno di uffici, aeroporti, sale d'aspetto in ospedali, e centri commerciali.

Ma la mia principale obiezione non riguarda il potenziale totalitario dei documenti d'identità nazionali, e nemmeno la probabilità che essi creino un'intera ed immensa nuova classe di disorganizzazione sociale ed economica. E non riguarda neanche il colossale spreco di tempo e di lavoro che questi documenti genereranno ai danni dei fornitori governativi. La mia obiezione contro una carta d'identità a livello nazionale, almeno nell'ambito di questa sede, è molto più semplice.

Non funzionerà. Non ci renderà più sicuri.

Infatti, tutto ciò che ho appreso in materia di sicurezza negli ultimi 20 anni mi dice che una volta messo in pratica, questo progetto per realizzare documenti d'identità nazionali finirà col renderci meno sicuri.

Il mio discorso può non risultare tanto ovvio, ma non è neanche difficile da seguire. Si incentra sul concetto secondo cui la sicurezza deve essere valutata non basandosi su come funziona, ma su come fallisce.

Non ha davvero molta importanza quanto bene funzioni una carta d'identità se usata dalle centinaia di milioni di persone oneste che l'avranno con sé. Ciò che importa è come il sistema possa fallire se utilizzato da qualcuno intenzionato a sovvertirlo: importa come il sistema fallisce naturalmente, come può essere indotto a fallire, e come possono essere sfruttati gli errori.

Il primo problema è rappresentato dalla carta stessa. La si può realizzare per essere il più possibile anti- contraffazione: verrà ugualmente contraffatta. Ancora peggio, alcuni individui otterranno documenti validi ma con nomi falsi.

Due dei terroristi dell'11 settembre avevano con sé delle patenti di guida dello stato della Virginia perfettamente valide ma sotto falso nome. Inoltre, anche se potessimo garantire l'assoluta incorruttibilità da parte di chi emette documenti d'identità nazionali, l'identità iniziale del possessore di tali documenti sarebbe determinata da altri documenti d'identità... ognuno dei quali sarebbe più semplice da contraffare.

Non ci sarebbe nemmeno un'unica carta d'identità. Attualmente viene smarrito in un anno circa il 20% di tutti i documenti d'identità. Un sistema di sicurezza totalmente distinto dovrebbe venire sviluppato per chi smarrisce la propria carta, un sistema esso stesso passibile di abuso.

In più, un qualsiasi sistema di documenti d'identità è legato alle persone... e le persone commettono regolarmente degli errori. Ognuno di noi conosce qualche barista che si è fatto ingannare da documenti palesemente falsi, oppure sa di certi controlli un po' troppo approssimativi agli aeroporti o in edifici governativi. Non è semplicemente una questione di addestramento: controllare documenti d'identità è un compito estremamente noioso, e gli sbagli sono dietro l'angolo. Elementi biometrici come le impronte del pollice possono essere promettenti, ma ci giungono con tutta una serie di problemi ad essi specifici.

Ma il problema primario legato a qualsiasi sistema di documenti d'identità è che viene richiesta la presenza di un database. In questo caso dovrebbe essere un database gigantesco contenente informazioni private e dati sensibili di ogni cittadino americano -- un database accessibile ovunque e istantaneamente, dai posti di controllo negli aeroporti, alle volanti della polizia, alle scuole, e così via.

I rischi di sicurezza sono enormi. Un simile database sarebbe composto da un'accozzaglia di altri database già esistenti riuniti alla meno peggio; database incompatibili, pieni di dati errati, e inaffidabili. In qualità di scienziati informatici, non sappiamo come rendere sicuro un database di queste dimensioni, non sapremmo come proteggerlo né dall'esterno (hacker), né dall'interno (le migliaia di persone autorizzate all'accesso).

Quando arrivano gli inevitabili worm, virus, o quegli errori casuali, che mettono in ginocchio il database, che si fa? L'America chiude baracca finché non viene ripristinato il tutto?

I fautori dei documenti d'identità nazionali pretendono che noi ci facciamo carico di tutti questi problemi, e le decine di miliardi di dollari che un tale sistema viene a costare, a che servono? A promettere di essere in grado di identificare qualcuno?

Quali benefici avrebbe portato il conoscere i nomi di Timothy McVeigh, dell'Unabomber, o dei cecchini di Washington prima che tutta questa gente venisse arrestata? Quei palestinesi kamikaze che si fanno saltare per aria in genere non hanno precedenti terroristici. Qui lo scopo è conoscere le intenzioni di qualcuno, e il conoscerne l'identità c'entra ben poco.

Esistono dei benefici di sicurezza nel possedere tutta una serie di diversi documenti di identità. Un'unica carta d'identità nazionale è un documento estremamente prezioso, e di conseguenza esistono maggiori incentivi a contraffarlo. C'è una maggiore sicurezza in guardie sveglie, che prestano attenzione a sottili indizi sociali, che non in guardie annoiate e al minimo sindacale che controllano pedissequamente i documenti.

Ecco perché, quando qualcuno mi chiede di stabilire la sicurezza di una carta d'identità nazionale in una scala da uno a dieci, non so mai rispondere. Non appartiene nemmeno ad una scala.

Questo intervento è apparso originariamente nel Minneapolis Star Tribune:
< <http://www.startribune.com/stories/1519/4698350.html> >

L'articolo di Kristof sul New York Times:
< <http://www.nytimes.com/2004/03/17/opinion/17KRIS.html?ex=1394946000&en=938b60e9bd051f7&ei=5007&partner=USERLAND> > oppure < <http://tinyurl.com/26fg2> >

Il mio precedente articolo sui documenti d'identità nazionali:
< <http://www.schneier.com/crypto-gram-0112.html#1> >

Il mio articolo sull'identificazione e la sicurezza:
< <http://www.schneier.com/crypto-gram-0402.html#6> >
< <http://www.cryptogram.it/febbraio04.htm#a6> > (versione in italiano)

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

Serrature autorizzate dalla TSA

Tempo fa, nel 1993, l'amministrazione Clinton propose di adottare il cosiddetto Clipper Chip. Il governo era preoccupato dal fatto che i criminali potessero iniziare a servirsi della crittografia, così venne ideata una soluzione. Il Clipper Chip avrebbe offerto una crittografia forte che non si sarebbe potuto decifrare, ma esisteva una chiave segreta -- conosciuta solo dal governo -- che avrebbe potuto decodificare il traffico. In quel modo gli utenti legittimi sarebbero stati al sicuro, e allo stesso tempo il governo sarebbe stato in grado di leggere i messaggi dei malintenzionati

Come immaginerete, è stata un'idea di scarso successo.

Alle persone non piaceva l'idea che il governo avesse una backdoor nella loro crittografia. Esperti come il sottoscritto non credevano che la backdoor sarebbe rimasta segreta e non pensavano che una crittografia deliberatamente limitata fosse una buona idea. Il concetto generale, conosciuto come key escrow, key recovery, o crittografia di terza parte fidata, è rimasto in circolazione qualche anno e poi è stato dimenticato.

Chi avrebbe mai pensato che sarebbe ricomparso sotto forma di una serratura per bagagli?

A partire dall'11 settembre, gli ufficiali di sicurezza degli aeroporti hanno iniziato ad aprire i bagagli molto più di frequente. Se trovano una valigetta chiusa a chiave, rompono la serratura. Ma alcuni viaggiatori abitualmente chiudono a chiave le proprie valigette, sia perché non vogliono che si aprano accidentalmente durante il viaggio, sia perché non vogliono che vengano aperte da qualche addetto ai bagagli in cerca di qualcosa da sgraffignare. Nel tentativo di soddisfare entrambe le esigenze, ora esiste una serratura "key escrow". Così voi potete chiudere a chiave ed aprire normalmente la vostra valigetta, ma vi è poi una chiave speciale della TSA che permette l'apertura anche agli ufficiali di sicurezza.

Vi sono due ragioni del perché si tratta di qualcosa di diverso. Anzitutto, non esiste un'altra possibilità: o si utilizza una di queste speciali chiusure, o si lascia la valigetta sbloccata. In questo caso, la soluzione può essere sempre meglio di niente.

In secondo luogo, è solo una valigetta. Non stiamo cercando di difenderci da un criminale che vuole squarciarla con un coltello o rubarla del tutto. Ci stiamo difendendo da qualche opportunista che vuole infilarsi le mani per rubacchiare qualcosa.

Certo, i "cattivi" otterranno copie delle chiavi speciali della TSA, e saranno in grado di aprire la vostra valigetta, ma del resto erano già in grado di scassinare le precedenti serrature, se volevano.

Io non ho mai chiuso a chiave la mia ventiquattrore, nemmeno quando ho viaggiato nel Terzo Mondo. I rischi mi sembrano minimi. Ma se qualcuno è preoccupato per la propria valigetta, mi sento di consigliare questa serratura. In questo caso, un pò di scena e un pò di sicurezza vera mi sembrano una buona combinazione.

Il sito Web della serratura:

< <http://www.travelsentry.org/travelers.htm> >

Le news a riguardo:

< http://www.pittsburghlive.com/x/tribune-review/news/s_172071.html >

< <http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2003/12/07/TRGM239RJB1.DTL> > oppure

< <http://tinyurl.com/2azte> >

Alcuni miei vecchi interventi sul recupero delle chiavi:

< <http://www.schneier.com/essay-infosec-scrambled-ft.html> >

< <http://www.schneier.com/paper-key-escrow.html> >

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

Le ristampe di Crypto- Gram

Crypto- Gram è attualmente al suo settimo 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.

Attacco automatizzato di tipo Denial- of- Service sfruttando le Poste USA:

< <http://www.schneier.com/crypto-gram-0304.html#1> >

< <http://www.cryptogram.it/aprile03.htm#a1> > (versione in italiano)

La precisione del database NCIC (National Crime Information Center)

< <http://www.schneier.com/crypto-gram-0304.html#7> >

< <http://www.cryptogram.it/aprile03.htm#a7> > (versione in italiano)

Naturalmente questa analisi è fatta col senno di poi. Nella pratica sarebbe necessario imbrogliare di più per essere sicuri di vincere. Ma anche così, i Democratici avrebbero potuto vincere cambiando meno dello 0,5% dei voti validi totali.

Ora proviamo a fare un'altra analisi: quanto può valere compromettere una macchina per il voto elettronico? Nella corsa alle elezioni camerali nel 2002, i candidati hanno speso in genere dai 3 ai 4 milioni di dollari, anche se il record è stato di 8 milioni. I risultati delle 20 corse elettorali più vicine sarebbero cambiati modificando una media di 2.593 voti per ognuna. Supponendo (per difetto) che un candidato sia disposto a pagare un milione di dollari per comprare 5.000 voti, ogni voto vale 200 dollari. Il valore vero e proprio si aggira molto più realisticamente sui 500 dollari, ma ho preferito rimanere su valori inferiori per tener conto anche del rischio aggiuntivo di violare la legge.

Se una macchina per il voto raccoglie 250 voti (circa 125 per ciascun candidato), manipolare la macchina per cambiare tutti quei voti costerebbe 25.000 dollari. Ma un quantitativo del genere non passerebbe inosservato, per cui è difficile che questo accada. Cambiare il 10% dei voti di ogni macchina costerebbe 2.500 dollari.

Ciò suggerisce come sia necessario presumere che eventuali attacchi ai danni delle singole macchine elettroniche per il voto siano un grave rischio.

Queste macchine sono dotate di software, il che vuol dire che occorre stabilire quanto valga compromettere il codice o l'architettura del software di una di queste macchine, e non solo le macchine stesse. Un qualsiasi tipo di macchina elettronica per il voto sistemata nel 25% dei distretti registrerebbe abbastanza voti da permettere a un software maligno di variare l'equilibrio dei poteri senza creare anomalie statistiche clamorosamente evidenti.

Nel 2002 tutti i candidati al Congresso hanno insieme superato i 500 milioni di dollari. Di conseguenza, si può concludere che modificare l'equilibrio dei poteri nella Camera dei Rappresentanti costa almeno 100 milioni di dollari al partito che, altrimenti, perderebbe le elezioni. Perciò, quando si progetta la sicurezza del software delle macchine per il voto, bisogna presumere un aggressore con un budget di almeno 100 milioni.

Conclusione: i rischi a cui sono sottoposte le macchine per il voto elettronico sono ancora maggiori di quanto sembra ad una prima analisi.

Questo articolo è stato scritto insieme a Paul Kocher.

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

Le news di Counterpane

Schneier interverrà alla CSO Perspectives Conference a San Diego il 19 aprile.
< <http://www.csoonline.com/perspectives/april2004/> >

Counterpane espone a NetWorld + Interop, che avrà luogo al Convention Center di Las Vegas dall'11 al 13 maggio. Visitateci allo stand 2021.

Counterpane ha sponsorizzato un webcast con Gartner. Sia Gartner che Counterpane parleranno di sicurezza di rete e di Managed Security Services.
< <http://www.accelacomm.com/jlp/cryptogram/0/10001788/> >

Altre recensioni di "Beyond Fear":
< <http://netsecurity.about.com/cs/bookreviews/gr/aapr032104.htm> >

< <http://victoria.tc.ca/int-grps/books/techrev/bkbyndfr.rvw> >
< <http://www.securitymanagement.com/library/001598.html> >

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

Note di sicurezza da ogni dove: il "Man- in- the- Middle Attack"

L'espressione "man- in- the- middle attack" viene usata per descrivere un attacco informatico in cui l'aggressore si trova nel punto medio del canale di comunicazione fra due persone, ingannandole entrambe. È un attacco molto serio, e genera ogni tipo di considerazioni progettuali in materia di protocolli di comunicazione.

Ma si tratta anche di un attacco che avviene nella vita reale. Prendiamo questa storia, di una donna che inserisce un annuncio facendo richiesta di una bambinaia. Quando una potenziale candidata al posto risponde, questa donna le chiede, per sicurezza, la sua serie di referenze. Poi inserisce un altro annuncio, utilizzando queste referenze come identità fasulla. Ottiene il posto come bambinaia con le referenze buone (sono vere, infatti, ma appartengono a un'altra persona), e poi deruba la famiglia che l'ha assunta e in seguito ripete il procedimento.

Osserviamo che cosa accade qui. Questa donna si inserisce nel mezzo di una comunicazione fra la vera bambinaia e il vero datore di lavoro, facendo finta di essere l'uno per l'altro. La vera bambinaia invia le proprie referenze a qualcuno che lei crede essere un potenziale datore di lavoro, non rendendosi conto che invece si tratta di un criminale. Il vero datore di lavoro, poi, riceve le referenze (vere) e le controlla, non rendendosi conto che di fatto non appartengono alla persona che le ha inviate.

È un reato davvero insidioso.

< <http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2004/03/18/BAG6S5MUEO1.DTL> >
oppure < <http://tinyurl.com/333dj> >

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

BeepCard

BeepCard è un'azienda che opera nella tecnologia, e commercializza un autenticatore sonoro per carte di credito. Il facsimile dimostrativo è in tutto e per tutto identico a una carta di credito, una vera carta di credito che risponde a tutti i requisiti di piegatura, affidabilità, ecc. e contiene un piccolo altoparlante e un chip sonoro. Quando una certa parte della carta viene premuta (il "pulsante"), essa emette una stringa sonora casuale a 128 bit perfettamente udibile.

Si tratta di una stringa non ripetibile che viene riprodotta per il software che sta all'altro capo della comunicazione, in modo simile a una SecurID card, per cui un aggressore non può registrare una stringa udibile e dedurne il resto.

Questa è forse una delle idee di sicurezza più carine che abbia mai visto da molto tempo a questa parte. L'azienda ha un'applicazione demo mediante la quale si è diretti ad un sito Web per acquistare qualcosa con carta di credito. Per autenticare la transazione, bisogna avvicinare la carta al microfono del proprio computer e premere il pulsante. Il suono viene catturato utilizzando un'applicazione Java o un controllo ActiveX -- non servono plug-in -- e funge da autenticatore. Dà prova, cioè, che la persona che sta effettuando l'acquisto non solo conosce il numero della

carta di credito, ma la sta tenendo effettivamente in mano. Nel linguaggio delle carte di credito, cambia lo stato della transazione da "carta assente" a "carta presente".

Cosa ancora più interessante, BeepCard sta apportando delle migliorie al sistema per fare in modo che la carta possieda anche un piccolo microfono. Questo sistema richiederà all'utente di dire una password ad alta voce prima di premere il pulsante sulla carta.

Perché mi piace tutto questo? Perché si tratta di un sistema fisico di autenticazione che non necessita di nessun hardware specifico per la lettura. Perché si può usare su un qualsiasi computer di un Internet point. Perché si può usare via telefono. Perché si possono pensare centinaia di usi diversi, in maniera semplice ed efficiente. Se il prodotto finale non sarà troppo costoso, BeepCard avrà sicuramente un buon successo.

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

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

Falla di sicurezza nel protocollo Bluetooth

Pare che i telefoni cellulari dotati di Bluetooth siano vulnerabili allo "snooping"; in altre parole, non è possibile tracciare le conversazioni, ma si può accedere ai contenuti dei telefoni stessi.

La falla è stata scoperta da Adam Laurie, un ricercatore di sicurezza del Regno Unito. Il London Times ne ha parlato l'altro giorno. L'hack viene chiamato "Bluesnarfing", e permette ad un hacker di scaricare in remoto l'elenco dei contatti, degli appuntamenti e delle immagini contenute nei telefonini Bluetooth compatibili.

Non sono in possesso dei dettagli tecnici, ma le implicazioni sono piuttosto gravi. Sarebbe infatti possibile andare a una fiera con il proprio computer portatile e scaricare gli elenchi dei contatti dei rappresentanti dei vostri concorrenti direttamente dai loro cellulari. Sarebbe possibile andare ad una conferenza stampa del Congresso e scaricare informazioni dai cellulari dei membri del Congresso. Questa storia è saltata fuori nel Regno Unito: so quanto piacerebbe ai reporter conoscere i nominativi presenti nelle rubriche telefoniche di Tony Blair o del Principe Carlo.

Non è chiaro quanti telefoni siano colpiti, se si tratta di un problema del protocollo Bluetooth stesso oppure se è solo un problema limitato all'implementazione del protocollo su determinati cellulari, né se il problema è rimediabile. Ma si tratta comunque di un bel guaio. Le persone trattano i propri cellulari come portafogli: ci mettono tutti i tipi di dati sensibili. Il fatto che qualcun altro abbia la possibilità di scaricare in remoto i contenuti di un telefonino è inquietante e fastidioso.

Gli articoli a riguardo (l'accesso è a pagamento):

< <http://www.timesonline.co.uk/article/0,,2-1073484,00.html?submit.x=47&submit.y=6> >

< <http://www.timesonline.co.uk/printFriendly/0,,1-7-1072761,00.html> >

Il mio articolo del 2000 sulla sicurezza del protocollo Bluetooth:

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

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

News

È possibile, e persino facile, utilizzare Google per cercare computer vulnerabili da attaccare. Ecco alcune delle possibilità:

< <http://johnny.ihackstuff.com/index.php?module=prodreviews> >

Ancora una volta, la corte ha imposto al Dipartimento dell'Interno degli Stati Uniti di scollegare i loro computer da Internet perché non era possibile salvaguardare i dati personali in essi contenuti:

< <http://www.techweb.com/wire/story/TWB20040317S0005> >

Siete preoccupati che le fotocamere automatizzate scattino una foto della targa della vostra auto quando passate col rosso? Questa compagnia commercializza una copertura per targhe che ne rende difficoltosa la lettura ad angolazioni superiori ai cinque gradi. Non è certo però se sia legale farne uso...

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

Una falla di sicurezza alla Equifax Canada ha permesso la diffusione di dati personali di circa 1.400 persone. I malfattori "facevano finta di essere dei legittimi concedenti di credito". A me sembra proprio un attacco non- tecnologico.

< <http://www.cbc.ca/stories/2004/03/16/canada/creditheft040316> >

< http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/1079408743242_24/?hub=TopStories >

oppure < <http://tinyurl.com/2ejcr> >

La risposta di Equifax Canada:

< http://www.equifax.com/EFX_Canada/news_and_perspective/press_e.html#Securitybreach >

oppure < <http://tinyurl.com/3aeht> >

CSO Magazine giudica la sicurezza delle informazioni governative.

< <http://www.csoonline.com/read/020104/grade.html> >

Qui si può trovare la vicenda di un uomo che ha volato dal Regno Unito all'Italia e ritorno, e a cui è stato controllato il passaporto svariate volte. Però egli aveva erroneamente preso il passaporto di sua moglie. Nessuno ci ha fatto caso.

< <http://news.bbc.co.uk/1/hi/england/oxfordshire/3495299.stm> >

Le quattro maggiori aziende contabili, più una compagnia di assicurazioni, stanno lavorando congiuntamente ad una struttura per la gestione dei rischi legati alla cyber- sicurezza. Potrebbe rivelarsi interessante.

< <http://www.computerworld.com/securitytopics/security/story/0,10801,91450,00.html?nas=SEC-91450> > or < <http://tinyurl.com/2huxo> >

Gli attivisti politici sono sulla "no fly- list" del Governo degli Stati Uniti:

< <http://www.commondreams.org/headlines02/0927-01.htm> >

< http://www.truthout.org/docs_04/020904E.shtml >

Ad alcuni sportelli Bancomat (in Texas) sono state applicate delle attrezzature per rubare i codici e i PIN delle carte di debito:

< <http://www.utexas.edu/admin/utpd/atm.html> >

Un interessante articolo riguardante le tecniche anti- contraffazione nelle banconote. L'autore esprime sorpresa per il fatto che il grande pubblico non controlli molto l'autenticità delle banconote. Secondo me, è perfettamente sensato. Non è fra i maggiori interessi di nessuno trovare banconote false nel proprio portafoglio. Una qualsiasi tecnologia anti- contraffazione che si appoggia su un controllo del denaro da parte dei cittadini è destinata a fallire, semplicemente perché la gente non lo farà. Ora, se le banche dessero una ricompensa pari a una volta e mezza il valore della banconota falsificata, allora i cittadini diventerebbero bravissimi a scoprire soldi falsi. Ma ciò porterebbe a tutta un'altra serie di problemi.

< <http://www.rbnz.govt.nz/currency/money/0116878.html> >

Banche e governi hanno bisogno di rilevare le falsificazioni:

< <http://www.bis.org/press/p040309.htm> >

Le regole sull'uso delle immagini del denaro in vari paesi del mondo:

< <http://www.rulesforuse.org> >

Un sedicente malato di mente ha dato un allarme bomba telefonico e ha impedito il decollo di un aereo. Immagino che non sia necessario essere dei terroristi per portare scompiglio alle linee aeree.

< <http://www.cnn.com/2004/US/West/03/27/psychic.plane.ap/index.html> >

< <http://www.mercurynews.com/mld/mercurynews/8293055.htm> >

Citando fonti anonime nella comunità dell'intelligence britannica, il Sunday Times ha riportato che un messaggio e-mail intercettato da spie della NSA ha accelerato una smisurata indagine antiterrorismo.

< <http://www.globetechnology.com/servlet/story/RTGAM.20040406.gterror06/BNStory/Technology/> > oppure < <http://tinyurl.com/2675t> >

Un'intervista interessante a Gene Spafford:

< <http://grop.law.harvard.edu/article.pl?sid=04/04/05/0353235&mode=nested> >

oppure

< <http://tinyurl.com/2yhgd> >

Interessante, seppur lungo, intervento sullo spam:

< http://www.colinfahey.com/spam_topics/spam_the_phenomenon.htm >

Un paio d'anni fa scrissi in merito ai problemi di sicurezza derivanti dall'armare i piloti degli aerei di linea. Ecco una storia molto interessante legata a quell'argomento. Un ufficiale di volo ha accidentalmente lasciato la propria rivoltella in una toilette dell'aeroporto... all'interno della sicurezza. Niente di eccezionale. Le probabilità che un terrorista abbia potuto trovare e usare l'arma sono praticamente zero. Le probabilità che un pazzo qualsiasi abbia potuto trovare e usare l'arma sono maggiori, ma sempre vicine allo zero. Ma la vicenda insegna che anche i sistemi di sicurezza progettati al meglio possono talvolta fallire.

< <http://www.reuters.com/newsArticle.jhtml?type=topNews&storyID=4803867> >

oppure < <http://tinyurl.com/38kbv> >

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

Le guerre dei virus

Ci troviamo nel mezzo di una enorme epidemia di worm e virus. Nelle scorse settimane ne sono stati trovati a decine e tutti di natura differente. La maggior parte di essi non sono nuovi, ma varianti di altri worm/virus.

Pare che vi sia una guerra continua fra gli autori del worm Bagle e gli autori del worm Netsky. Molte varianti di ciascuno dei due stanno circolando in Internet e sembra che in ogni momento ne salti fuori una nuova. Nelle varie versioni sono incorporati dei commenti e delle frecciate di un partito ai danni dell'altro.

Ad esempio, ecco quel che è stato trovato in Netsky.R: "Sì, certo, lo avete capito. Bagle è uno stronzo, apre una backdoor, e fa un sacco di soldi. Netsky no. Netsky è Skynet, un buon software, c'è brava gente dietro, che ci crediate o no. Rilascieremo migliaia di varianti del nostro Skynet, finché ci sarà in giro Bagle e quelli che l'hanno scritto... Grazie a Bruce Schneider e a tutta la gente nella Repubblica Ceca e in Russia. Tanti saluti. Noi siamo l'unico vero Skynet."

(Sì, ho usato questo esempio perché fanno il mio nome).

Da quel poco che posso giudicare dal loro sito e dalle e-mail inviate ai loro rappresentanti per le vendite, Symbiot è governata da un branco di idioti. Ma quel che sembra vogliono ottenere è l'autodifesa. Fermare cioè la persona che sta cercando di farci del male, eliminando la sua capacità di recare danni nel momento in cui sta cercando di colpire.

La differenza è molto importante ed è stata un'istituzione di legge da tempo immemore.

Nella mia seconda vita, quella in cui non scrivo software e non amministro macchine Linux, faccio molte cose che riguardano l'autodifesa -- tengo corsi di autodifesa per donne, aiuto donne che hanno subito abusi ad uscire da situazioni pericolose, insegno ad usare armi da fuoco, ottengo certificazioni in qualità di consulente tecnico in casi di autodifesa e di uso di forza... quel genere di cose.

Nel mondo di tutti i giorni, le problematiche sono molto chiare e semplici da capire. Puoi colpirlo per far sì che lui smetta di colpirti. Puoi bloccarlo finché non arriva la polizia. Non puoi colpirlo se egli non rappresenta una minaccia immediata. Non puoi continuare a colpirlo se lui ha smesso di colpirti. E di sicuro noi puoi colpirlo una volta di troppo solo perché se lo merita.

Nel mondo fisico e psicologico esiste un altro principio: la deterrenza. A grandi linee, la sicurezza fisica e la protezione sono un processo comunicativo. In qualità di difensore, occorre comunicare con l'aggressore in un linguaggio che possa comprendere, e che gli possa far capire che qualunque cosa voglia non vale quanto dovrà pagare per ottenerla. Se lei ha mai posseduto cani o gatti, saprà certamente a cosa mi riferisco.

Per cui, se separiamo le due problematiche, ritengo che vi sia qualcosa di legittimo in atto. La deterrenza si basa sui costi percepiti. Le classiche misure di sicurezza sono generalmente passive: aumentano il lasso di tempo necessario ad un criminale per ottenere ciò che vuole.

Le sanzioni penali aiutano. Processi molto pubblicizzati e conclusi con multe salate o sentenze di incarcerazione faranno sicuramente in modo che molti "black hat" ci pensino due volte prima di agire. Ma la legge, come qualsiasi poliziotto vi dirà, non agisce: se mai reagisce dopo il fatto. E non può fare nulla contro attacchi partiti da paesi esteri.

Gente come quelli di Symbiot reagiscono, a quanto mi è dato vedere, non solo al desiderio di vendetta. È il riconoscimento di ciò che tutti noi, nel profondo, sappiamo sull'autodifesa e sulla deterrenza. Stanno affrontando una reale preoccupazione, anche se goffamente e sono consapevoli (anche se non lo sono) di quel che può essere una debolezza irrimediabile nella sicurezza elettronica.

Da: Drew Johnson <a2johnson@yahoo.co.uk>

Oggetto: Centralizzazione e benefici per la sicurezza

Ritengo che sia stata una buona idea il cercare di dare un modello dell'economia della centralizzazione della sicurezza (Crypto-Gram del 15 marzo 2004), ma vorrei aprire un dibattito sulle sue conclusioni. Nella realtà, le spese per investire sulla sicurezza sono vincolate. Tenendo presente questo aspetto, credo che l'opposto sia vero: centralizzare è una buona cosa!

Riconsideriamo i due scenari ammettendo che io debba proteggere 1000 dollari avendo soltanto un budget per la sicurezza limitato a 10 dollari.

Scenario 1:

Mi rivolgo a un produttore e compro dieci cassette di sicurezza virtuali da 200 dollari l'una e che mi costano 1 dollaro l'una. In ognuna di esse ci metto 100 dollari. Un aggressore qualsiasi avrà bisogno del flusso di cassa necessario per trovare 200 dollari anticipati se intende lanciare un

attacco. Dopo aver attaccato con successo la prima cassetta, l'aggressore è sotto di 100 dollari. Tuttavia, dato che i computer su cui si trovano le cassette di sicurezza virtuali hanno le stesse vulnerabilità, lo stesso attacco può essere ripetuto al minimo costo marginale (cioè 1 dollaro). Perciò, dopo aver attaccato la terza cassetta, l'aggressore è sopra di 98 dollari.

Dopo aver attaccato tutte le dieci cassette, l'aggressore avrà un profitto di 791 dollari, mentre io ne avrò persi 1010.

Scenario 2:

Spendo il mio intero budget di 10 dollari in una cassetta di sicurezza virtuale da 500 dollari e ce ne metto 1000. (Si noti che, almeno all'inizio, sembra che si dia meno valore ai soldi; ogni dollaro ne compra 50 per la protezione, mentre nello scenario 1 ne comprava 200.) Ora la barriera d'ingresso per l'aggressore è stata alzata a 500 dollari. Un qualsiasi aggressore dovrà anche considerare i rischi operativi riguardanti l'attacco. La cassaforte da 500 dollari potrebbe avere dei meccanismi migliori per il tracciamento e la prosecuzione dei malfattori.

In caso di successo, l'aggressore avrà un profitto di 500 dollari, mentre io ne perdo ancora 1010.

E dunque in quali modi l'aver centralizzato la sicurezza (con un budget prefissato) ha influito sui rischi?

L'impatto è identico in entrambi gli scenari, ma la probabilità è stata diminuita nello scenario 2. Questo perché è aumentato il costo iniziale per l'attacco (diminuendo così il numero di aggressori) e sono stati smorzati gli incentivi per un aggressore diminuendo il profitto e possibilmente aumentando i rischi di un rilevamento.

Io so come spenderei il mio budget.

Da: "A. L. Papadopoulos" <dp949@tutor.open.ac.uk>

Oggetto: V-ID

Questo sistema è aperto a ogni genere di abusi e incompetenze. Per quanto concerne l'abuso, non sono convinto che chiunque abbia accesso a informazioni potenzialmente intimidatorie si esimerà dall'usare tali informazioni abusivamente, mediante ricatti, settarismo, speculazione, e così via. Impiegati scorretti potrebbero creare falsi negativi così come falsi positivi. Ciò è confermato dalla vicenda legata alle agenzie di background check nel Regno Unito, dove è attualmente in corso uno scandalo in merito alle gravi incompetenze della compagnia che gestisce i background check. Non ho trovato la pagina che descrive in dettaglio il caso di alcuni insegnanti erroneamente identificati come criminali e a cui è stato negato un posto di lavoro, per cui non ne reclamerò la veridicità, ma vi sono tantissimi articoli sul Bureau del Registro Criminale del Regno Unito, e su un provider IT chiamato Capita, tutti dello stesso tono.

Credo che questi due fattori -- abuso e incompetenza -- siano un motivo sufficiente per rigettare un qualsiasi sistema che si affida sulle strategie della V-ID come sono state riportate.

Da: "Bruce Kaalund" <bakaalund@comcast.net>

Oggetto: Tessere che certificano "Io non sono un Terrorista"

Ecco un altro caso che oppone chi ha e chi non ha. Il fatto che qualcuno sia in possesso di una carta che "comprova" che costui non è un terrorista, non solo sarebbe un mezzo per far sì che i potenziali malfattori possano introdursi nel sistema, ma finirebbe col generare un maggior numero di sospetti. Siccome occorre pagare per avere la tessera, si corre il rischio di far diventare i meno abbienti un bersaglio ancora più evidente per le forze dell'ordine. E in più ci sono i viaggiatori occasionali, o tutti quelli che vanno allo stadio una sola volta all'anno, a causa del costo

del biglietto. E per quanto non ci piaccia parlarne, un tale sistema finirebbe con l'etichettare come potenziali terroristi tutti coloro che sono già ai margini della società (da un punto di vista etnico, razziale, sociale e/o economico). Queste persone ora diventano i membri del XXI secolo del grande gruppo dei "sans papiers", dei senza documenti. Chi deve viaggiare per lavoro si prenderà la tessera, perché la sua azienda ne pagherà i costi. Queste persone tendono ad appartenere allo stato dei più economicamente privilegiati, che copre sì le varie categorie etniche e razziali, ma non al punto di essere davvero neutrale. Sono certo inoltre che i fautori delle libertà civili solleveranno gravi preoccupazioni a riguardo.

Da: Nicholas Weaver <nweaver@ICS.Berkeley.EDU>

Oggetto: Il codice sorgente Microsoft e la sicurezza...

Dobbiamo assumere che un aggressore davvero competente abbia già accesso al codice sorgente di Windows. I governi russo e cinese hanno accesso legittimo, e di conseguenza i loro servizi di intelligence. Un interessante esercizio di pensiero legato a questo argomento sarebbe quello di calcolare quanto costerebbe a un'organizzazione criminale il tentare di sottrarre a Microsoft la copia più recente del codice sorgente.

L'accesso fisico sembra una tattica ovvia, e probabilmente basterebbero alcune centinaia di dollari per corrompere un addetto alle pulizie e una chiave USB a lui affidata per ottenere un piccolo punto d'appoggio all'interno della rete. Anche attacchi di rete sembrano plausibili, soprattutto attacchi IE. Basta attaccare un grosso server di banner pubblicitari e, invece di agire indiscriminatamente, rispondere con un Trojan solo ad indirizzi IP di proprietà di Microsoft. In entrambi i casi, il rischio di cattura è ragionevolmente basso, il costo in termini di tempo viene misurato in mesi-uomo o meno, e il costo in dollari è irrilevante.

Così, in tutti i casi, il motto è chiaro: DOBBIAMO assumere che i criminali veri sono in possesso dell'ultima versione del codice sorgente Windows, se ritengono che possano trarne dei benefici. Non è un pensiero rassicurante, specie se lo uniamo all'osservazione che Windows è una Infrastruttura Critica.

Da: "Ian D. Eccles" <ide101@psu.edu>

Oggetto: L'Economia dello spam

Nel numero di Febbraio di Crypto-Gram, lei ha pubblicato un articolo dal titolo "L'Economia dello Spam". Ha ragione nell'affermare che gli spammer rispondono alla chiusura dei loro account utilizzando altri account rubati. Proprio per questo motivo, credo fortemente che il terzo punto di Bill Gates sia forse il più debole. Se da un lato obbligare qualcuno a pagare per le e-mail che spedisce può imporre un fortuito controllo qualità sul messaggio inviato, ciò può funzionare solo nel caso in cui la persona che invia l'e-mail è la stessa che ha pagato. Presumibilmente, qualsiasi tipo di sendmail che permette una fatturazione, avrà una qualche forma di autenticazione (molto probabilmente nome-utente/password associati ad un account). Se questo rende più difficile rubare degli account, di certo non lo rende impossibile, né tantomeno irrealizzabile; le password vengono rubate molto di frequente. Per cui, se l'account e-mail di Alice viene craccato da Bob, il quale poi invia e-mail spazzatura a tutto il mondo pubblicizzando il suo nuovo prodotto "per aumentare le prestazioni maschili", Alice potrebbe essere quella che poi paga il conto. In questo modo per Bob fare dello spam è comunque rimasto gratuito, ma non per Alice. L'economia dello spam sembra peggiore in questo caso perché Alice ha pagato un servizio che non ha utilizzato. Certo, dato che esiste una fattura, è più probabile che Alice presenti un reclamo, e che riesca ad ottenere una qualche indagine che porti al vero colpevole. Tuttavia, se uno spammer attua la tattica di rubare moltissimi account e di spammare in misura limitata da ognuno di essi (e quindi non gravando molto sui costi dei malcapitati a cui è stato sottratto l'account), i danni potrebbero passare inosservati. In questo caso, fare spamming è ancora gratis per lo spammer.

