

CRYPTO-GRAM
15 giugno 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>.

Crypto-Gram è anche consultabile in formato RSS.

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

In questo numero:

Il valore della privacy
Concorso: Minaccia da Trama Cinematografica - Il vincitore
Le ristampe di Crypto-Gram
Diebold non comprende la minaccia alla sicurezza
News
Inserirsi illecitamente nei computer tramite USB
Il Canile: KRYPTO 2.0
Le News di Counterpane
Allineare l'interesse con la possibilità
Commenti dei lettori

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

Il valore della privacy

Il mese scorso la rivelazione di un ennesimo tentativo di sorveglianza della NSA ai danni dei cittadini americani ha riaperto il dibattito sulla privacy. Chi è a favore di programmi di questo genere ha tirato fuori la solita domanda retorica che si sente ogni volta che i difensori della privacy si oppongono ai controlli d'identità, alle telecamere di sorveglianza, ai database enormi, al data mining e ad altre misure di sorveglianza all'ingrosso: "Se non state facendo nulla di male, che cosa avete da nascondere?".

Alcune risposte intelligenti: "Se non sto facendo niente di male, allora non c'è ragione di osservarmi". "Perché è il governo a definire che cosa è male, e cambia questa definizione di continuo". "Perché potreste fare qualcosa di male con le informazioni che mi riguardano". Il mio problema con queste battute sagaci, per giuste che siano, è che accettano tutte la premessa per cui privacy significa nascondere qualcosa di male o di sbagliato. Non è così. La privacy è un diritto umano intrinseco, e un requisito per mantenere la condizione umana con dignità e rispetto.

Due proverbi spiegano il concetto ancor meglio: "Quis custodiet ipsos

custodes?" ("Chi sorveglierà i sorveglianti?") e "Absolute power corrupts absolutely" ("Il potere assoluto corrompe assolutamente").

Il Cardinale Richelieu comprese il valore della sorveglianza quando disse mirabilmente: "Datemi sei righe scritte dall'uomo più onesto, e ci troverò qualcosa per farlo impiccare". Si osservi qualcuno per un tempo abbastanza lungo, e si scoprirà qualcosa per cui farlo arrestare, o quantomeno per ricattarlo. La privacy è importante perché senza di essa le informazioni ricavate dalla sorveglianza verranno abusate: per spiare qualcuno, per rivenderle ai commercianti, e per spiare nemici politici, chiunque essi siano in quel momento.

La privacy ci protegge dagli abusi di chi detiene il potere, anche se non stiamo facendo niente di male mentre veniamo sorvegliati.

Non facciamo niente di male quando facciamo l'amore o andiamo al bagno. Non stiamo volontariamente nascondendo nulla di particolare quando cerchiamo un angolo tranquillo per riflettere o conversare. Teniamo diari privati, cantiamo nella privacy della doccia, scriviamo lettere ad amanti segreti per poi bruciarle. La privacy è un'esigenza umana essenziale.

Un futuro in cui la privacy avrebbe dovuto affrontare ripetuti attacchi e minacce era talmente estraneo agli artefici della Costituzione americana che non pensarono nemmeno di definire la privacy come un preciso diritto. La privacy era intrinseca alla nobiltà del loro essere e della loro causa. Ovviamente essere osservati nella propria dimora era assurdo. La semplice osservazione era un atto così indecente da risultare inconcepibile fra i gentiluomini di quell'epoca. Si tenevano sotto osservazione i criminali in prigione, non i liberi cittadini. Ognuno era padrone nella propria casa. È parte essenziale del concetto di libertà.

Perché se veniamo osservati in ogni cosa che facciamo, siamo costantemente esposti a correzioni, giudizi, critiche, persino al plagio della nostra unicità. Diventiamo bambini, incatenati e sotto continua osservazione, sempre col terrore che, oggi o in un futuro incerto, la trama di azioni che ci lasciamo alle spalle possa essere ripresa per implicarci, per mano di qualsiasi autorità ora concentrata su quelle azioni innocenti, che in passato erano anche private. Perdiamo la nostra individualità, perché tutto quel che facciamo è osservabile e registrabile.

Quanti di noi negli ultimi quattro anni e mezzo si sono fermati durante una conversazione, colti improvvisamente dal sospetto che qualcuno potesse essere in ascolto di nascosto? Magari era una conversazione telefonica, o uno scambio di email o di messaggi in chat, o una chiacchierata in un luogo pubblico. Magari si parlava di terrorismo, di politica o dell'Islam. Ci blocchiamo all'improvviso, temendo per un istante che le nostre parole possano essere decontestualizzate... Poi ridiamo della nostra paranoia e passiamo oltre. Ma il nostro comportamento è cambiato, e le nostre parole lievemente corrette.

Questa è la perdita di libertà che affrontiamo quando veniamo privati della nostra privacy. Questa era la vita nell'ex Germania dell'Est o nell'Iraq di Saddam Hussein. E sarà il nostro futuro se lasciamo che un "occhio" costantemente invadente entri a osservare la nostra vita privata.

In troppi definiscono il dibattito secondo la linea "sicurezza in opposizione alla privacy". La vera scelta è invece libertà in opposizione al controllo. La tirannia, che si sviluppi dalla minaccia di un attacco straniero o dalla continua sorveglianza interna da parte

delle autorità, è sempre tirannia. La libertà richiede la sicurezza senza intrusione: sicurezza PIÙ privacy. L'onnipresente sorveglianza da parte delle forze dell'ordine è la pura e semplice definizione di uno stato di polizia. Ed è per questo che dovremmo difendere la privacy anche quando non abbiamo nulla da nascondere.

Una versione di questo articolo è originariamente apparsa su Wired.com.
<<http://www.wired.com/news/columns/0,70886-0.html>>

Il commento di Daniel Solove:

<http://www.concurringopinions.com/archives/2006/05/is_there_a_good.html>

oppure <<http://tinyurl.com/nmj3u>>

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

Concorso: Minaccia da Trama Cinematografica - Il vincitore

Posso dirvi una cosa: voi altri avete una grandissima inventiva. La risposta che ha ricevuto il mio Concorso "Minaccia da Trama Cinematografica" è stata ben superiore a quanto potessi immaginare: 892 commenti. Li ho stampati tutti (195 pagine, fronte e retro) e li ho rilegati a spirale, così da poterli leggere più comodamente. In copertina il titolo: "The Big Book of Terrorist Plots" ["Il Gran Libro delle Trame Terroristiche"]. Ho cercato di non mostrarlo troppo negli aeroporti.

Quasi non volevo scegliere un vincitore, perché di fatto vi sarebbe un lungo elenco di vincitori. E poi è difficile scegliere. Ma dopo attenta deliberazione, l'idea vincente è a firma Tom Grant. Sebbene l'uso di aerei pieni di esplosivo è già un cliché, distruggere la Diga Gran Coulee è un'idea geniale. Eccola:

"La Missione: Terrorizzare gli americani. Neutralizzare l'economia americana, far sentire l'America totalmente vulnerabile e far sentire i cittadini americani in pericolo.

"Scena 1. Un furgone noleggiato parte da Spokane, Washington, e si dirige in una remota località nell'Idaho. Lì vengono caricati lanciarazzi da spalla e salgono due persone vestite in uniformi da fatica.

"Scena 2. Terroristi vestiti in abiti da fattorino prendono il controllo del deposito merci UPS dell'aeroporto di Spokane, Washington. Un furgone pieno di esplosivi viene scaricato al deposito.

"Scena 3. Terroristi vestiti in abiti da fattorino prendono il controllo del deposito merci UPS dell'aeroporto di Kamloops, British Columbia. Un furgone pieno di esplosivi viene scaricato al deposito.

"Scena 4. Un furgone con a bordo dei mercenari si dirige, attraverso le foreste dell'Idaho, a una destinazione ignota. Riceve un comunicato ufficiale via cellulare che le postazioni Alpha e Bravo sono in posizione.

"Scena 5. Un aereo da carico UPS atterra a Kamloops e viene atteso al deposito da un gruppo di terroristi che prende il controllo dell'aereo e dell'equipaggio. Sull'aereo vengono caricati esplosivi. La stessa cosa viene attuata a Spokane poco dopo, e laggiù un secondo aereo viene riempito di esplosivi. Due piloti prendono il comando di ognuno dei due aerei e richiedono istruzioni per il decollo. La notte inizia a calare

nell'Ovest.

"Scena 6. Due aerei da carico prendono il volo da due diverse località. Un furgone con quattro terroristi giunge a destinazione, e viene parcheggiato su un crinale, in un punto d'osservazione, al calar della notte. I terroristi si servono di occhiali agli infrarossi per esaminare il bersaglio. La cinepresa si allontana dal van e fa una panoramica fino a mostrare il bersaglio: la Diga Gran Coulee. Suona il cellulare e al caposquadra viene comunicato che 'Gli uccelli notturni alpha e bravo hanno preso il volo'.

"Scena 7. Due operatori radar in due diverse località notano allarmati che gli aerei da carico UPS sono scomparsi dai radar e potrebbero essersi schiantati. A bordo dei due aerei i piloti hanno spento la navigazione radioassistita e stanno volando in 'manuale' a bassa quota. Uno verso Sud, l'altro verso Nord.

"Scena 8. Gli aerei si stanno avvicinando al 'bersaglio' e la squadra lanciarazzi si mette al lavoro. Con precisione colpiscono le posizioni di guardia e di difesa sulla diga, poi prendono di mira gli uffici più in basso. Non appena ultimato il lavoro, un aereo da carico si avvicina da Nord ad alta velocità, schiantandosi contro la parte posteriore della diga appena sopra la linea d'acqua ed esplodendo, facendo tremare la terra. Una grande porzione della parte medio-alta della diga viene spazzata via. Nel giro di pochi secondi un aereo da carico proveniente da Sud si schianta nella parte frontale della diga, più verso la base, ed esplosione facendo tremare la terra. Dopo poco, la diga comincia a cedere, e un'ultima raffica dei lanciarazzi dalla collina sovrastante aiuta ad aprire definitivamente la parte frontale della diga. Il Lago Roosevelt, lungo 40 miglia inizia a riversarsi nella Columbia River Valley, fuori controllo. Nessun preavviso viene dato alle altre dighe a fondovalle, se non che la Gran Coulee è ora senza energia.

"Scena 9. Durante la notte, il crescente muro d'acqua si infrange lungo la via d'acqua della Columbia, sovrastando una diga dopo l'altra, aumentando progressivamente in velocità e in massa d'acqua durante il tragitto. Le città di Wenatchee e Kennewick vengono travolte e spazzate via in gran parte. Un furgone di rinnegati si rifugia nell'Idaho del Nord.

"Scena 10. Quando arriva il giorno a illuminare l'Ovest, non c'è energia elettrica da Seattle a Los Angeles. La rete elettrica dell'intero Ovest non funziona. Il commercio si è arrestato a ovest delle Montagne Rocciose. L'acqua si sta muovendo rapidamente nella gola del Columbia River, minacciando la diga di Bonneville e l'intera area metropolitana di Portland, Oregon.

"Scena 11. Bin Laden trasmette un video su Al Jazeera dichiarando vittoria sugli americani.

"Scena 12. È il pandemonio quando la massa d'acqua si riversa in una Portland nel panico, travolgendo ogni cosa sul suo cammino e sollevando acqua su fino alla Willamette Valley.

"Scena 13. Stanza dei bottoni a Washington: scarsissime informazioni arrivano dall'Ovest. Alcune basi militari hanno generatori di emergenza e telefoni satellitari, e riportano che la devastazione dell'infrastruttura di dighe è totale. Sono state distrutte sette dighe maggiori e cinque minori. Ci vorranno mesi per ripristinare l'energia nella West Coast, dato che i collegamenti con la rete elettrica dell'Est dovranno essere effettuati attraverso le montagne del New Mexico.

"Scena 14. Il peggiore crollo del mercato USA che la storia ricordi. Il

Prodotto Nazionale Lordo degli Stati Uniti scende al 20° posto a livello mondiale. Cessano le esportazioni e le importazioni nella West Coast. La legge marziale non riesce a controllare l'esodo di massa da Seattle, San Francisco e Los Angeles - milioni di individui migrano verso est. La mancanza di carburante e la mentalità da vigilantes minano la popolazione impaurita. L'Ovest è 'selvaggio' ancora una volta. L'Est è invaso da milioni di persone in cerca di una casa e di un lavoro".

Complimenti, Tom. Sto ancora pensando a quale potrebbe essere il premio per te.

Le regole del concorso e i contributi:

http://www.schneier.com/blog/archives/2006/04/announcing_movi.html

L'aggiornamento, che comprende i criteri per la selezione:

http://www.schneier.com/blog/archives/2006/04/movie_plot_thre.html

Il contributo vincente:

http://www.schneier.com/blog/archives/2006/04/announcing_movi.html#c54905

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

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 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. (le corrispondenti traduzioni in italiano le potete trovare all' indirizzo <http://www.cryptogram.it/crypto-gram.html>, ndt).

Attacchi in Internet nel 2005: andamenti e tendenze:

<http://www.schneier.com/crypto-gram-0506.html#1>

Ridotta all'osso la legge sulla privacy sanitaria statunitense:

<http://www.schneier.com/crypto-gram-0506.html#9>

La scoperta dei codici iraniani:

<http://www.schneier.com/crypto-gram-0406.html#1>

Il worm Witty:

<http://www.schneier.com/crypto-gram-0406.html#9>

I rischi del cyber-terrorismo:

<http://www.schneier.com/crypto-gram-0306.html#1>

Rimediare agli insuccessi dell'intelligence:

<http://www.schneier.com/crypto-gram-0206.html#1>

Gli honeypot e il Progetto HoneyNet:

<http://www.schneier.com/crypto-gram-0106.html#1>

Microsoft e il protocollo SOAP:

<http://www.schneier.com/crypto-gram-0006.html#SOAP>

Il DES (Data Encryption Standard):

<http://www.schneier.com/crypto-gram-0006.html#DES>

L'internazionalizzazione della linea di condotta della crittografia:
<<http://www.schneier.com/crypto-gram-9906.html#policy>>
e dei prodotti:
<<http://www.schneier.com/crypto-gram-9906.html#products>>

I nuovi generi di virus, worm, e altro software maligno:
<<http://www.schneier.com/crypto-gram-9906.html#viruses>>

Timing attack, power analysis e altri attacchi di tipo "side-channel"
contro i criptosistemi:
<<http://www.schneier.com/crypto-gram-9806.html#side>>

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

Diebold non comprende la minaccia alla sicurezza

Questa citazione riassume molto bene le ragioni per cui non ci si dovrebbe fidare di Diebold per la sicurezza delle macchine per il voto elettronico:

"David Bear, un portavoce di Diebold Election Systems, ha dichiarato che il rischio potenziale era presente poiché i tecnici della compagnia avevano intenzionalmente costruito le macchine in modo tale da permettere agli ufficiali elettorali di aggiornare i propri sistemi negli anni a venire.

"Perché vi sia un problema qui, si deve sostanzialmente dare per assodata la premessa per cui vi siano ufficiali elettorali malevoli e corrotti che introducano un pezzo di software di nascosto", ha detto Bear. "Non credo esistano tali individui nei seggi elettorali".

Se non si è in grado di comprendere il modello di minaccia, è inutile sperare di proteggere il sistema.

<<http://www.nytimes.com/2006/05/12/us/12vote.html?ex=1305086400&en=5b3554a76aad524a&ei=5090&partner=rssuserland&emc=rss>> oppure
<<http://tinyurl.com/q7p4s>>

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

News

I consumatori sono disposti a cedere privacy in cambio di maggiori comodità:
<<http://www.computerworld.com.au/pp.php?id=42605808&eid=-180>>

Due conferenze:

The Workshop on Economics and Information Security [Laboratorio su Economia e Information Security], il 26-28 giugno a Cambridge (Inghilterra, non Massachusetts).
<<http://weis2006.econinfosec.org/>>

The Workshop on the Economics of Securing the Information Infrastructure [Laboratorio sull'economia della protezione dell'infrastruttura di informazione], 23-24 ottobre a Washington, DC.
<<http://wesii.econinfosec.org/>>

WEIS è al momento la conferenza sulla sicurezza che preferisco. Credo che l'economia abbia molto da insegnare alla sicurezza informatica, ed è molto interessante riunire economisti, avvocati ed esperti di sicurezza informatica nella stessa stanza a dibattere svariate problematiche.

Esami online. Sono certo che si tratta di una buona idea, ma mi chiedo quando accadrà il primo caso di imbroglio attraverso un rootkit.

<http://news.bbc.co.uk/go/rss/-/1/hi/scotland/4962806.stm>

Il Bundesamt für Sicherheit in der Informationstechnik (Ufficio Federale per l'Information Security), o BSI, è l'equivalente tedesco della NSA. Ha un sito Web in inglese che raccoglie diverse pubblicazioni in lingua inglese sulla sicurezza.

<http://www.bsi.bund.de/english/publications/index.htm>

Il NIST (National Institute of Standards and Technology) ha pubblicato un documento che illustra come le agenzie federali dovrebbero gestire i log di sicurezza: NIST Special Publication 800-92: Guide to Computer Security Log Management.

<http://csrc.nist.gov/publications/drafts/DRAFT-SP800-92.pdf>

Ottimo suggerimento passo per passo su come sopravvivere al furto d'identità:

<http://www.consumerist.com/consumer/top/how-to-get-through-having-your-identity-stolen-171194.php> oppure <http://tinyurl.com/hqksb>

Un nuovo rapporto del GAO: GAO-06-385, "The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information" [Il Governo Federale deve stabilire linee di condotta e procedimenti per condividere informazioni sensibili ma non segrete sul Terrorismo] del marzo 2006 elenca 56 differenti designazioni di sicurezza sensibili ma non segrete.

<http://www.gao.gov/htext/d06385.html>

L'elenco è qui:

http://www.schneier.com/blog/archives/2006/05/us_government_s.html

Ho già parlato delle SSI (Sensitive Security Information).

http://www.schneier.com/blog/archives/2005/03/sensitive_secur.html

La Guardia Costiera Statunitense sollecita gli sceneggiatori di Hollywood a venirle in aiuto con le minacce da trama cinematografica. Sul serio.

http://www.signonsandiego.com/uniontrib/20060520/news_1n20ships.html

Chiunque abbia visto ciò che Hollywood ha prodotto in questi ultimi anni sa che gli sceneggiatori non sono proprio la categoria più creativa del pianeta Terra.

Profiling intelligente da parte del Dipartimento per la Sicurezza Nazionale e della TSA: "Una selezione di dipendenti della TSA verrà addestrata all'identificazione di individui sospetti il cui comportamento, insolito o ansioso sia motivo di allarme. Semplici indizi di un tale comportamento possono essere cambiamenti nel modo di agire, sudorazione eccessiva in una giornata fresca, cambiamenti nel registro vocale". Era ora.

<http://www.time.com/time/nation/article/0,8599,1195330,00.html>

Degli spammer russi hanno attaccato l'azienda Blue Security, e Blue Security si è rassegnata alla disfatta.

<http://www.washingtonpost.com/wp-dyn/content/article/2006/05/16/AR2006051601873.html>

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

http://www.techweb.com/headlines_week/showArticle.jhtml?articleId=187900260 oppure <http://tinyurl.com/p9fb5>

<http://news.bbc.co.uk/2/hi/technology/4990622.stm>

Marcus Ranum a proposito dell'idea di Blue Security:

http://www.ranum.com/security/computer_security/editorials/bluesecurity/index.html oppure <http://tinyurl.com/qrhcf>

El Al non si fida della TSA e vuole occuparsi essa stessa della sicurezza:

<http://www.haaretz.com/hasen/spages/714988.html>

Grande editoriale di opinione sul perché il data mining non servirà a scovare terroristi:

<http://www.nytimes.com/2006/05/16/opinion/16farley.html?ex=1305432000&ei=5088&partner=rssnyt&emc=rss> oppure <http://tinyurl.com/nod9s>

L'autore è Jonathan Farley, professore di matematica ad Harvard.

http://www.math.buffalo.edu/mad/PEEPS/farley_jonathan.html

Vincitore del mio premio per la minaccia da trama cinematografica più stupida del mese, ecco qualcuno che crede che parti elettroniche fasulle siano uno strumento del terrorismo.

<http://spectrum.ieee.org/may06/3423/boguf4>

<http://www.cyberdefenseagency.com/news-20060531.php>

Secondo posto per il premio minaccia da trama cinematografica più stupida del mese, ecco qualcuno che crede che un sistema pubblico di tracciamento degli aerei sarebbe "il sogno di ogni terrorista".

<http://dailytelegraph.news.com.au/story/0,20281,19000724-5001028,00.html>

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

Con il sistema attuale, un terrorista può localizzare la posizione di un aereo semplicemente guardando in aria. E se un terrorista è abbastanza capace da effettuare questo esercizio di raccolta di intelligence nei pressi di un aeroporto, egli può individuare la posizione di aerei più prossimi a terra, e quindi più semplici da abbattere mediante missili. Perché ci stiamo preoccupando della possibilità di star comunicando ai terroristi dove si trovano gli aerei che viaggiano ad alta quota, e che sono più difficili da abbattere? Ovviamente posso sempre inventarmi una storia da film in cui i terroristi devono neutralizzare un certo aeroplano perché a bordo si trova questa o quella celebrità, ma sarebbe un po' troppo.

Uno spezzone del film "Team America: World Police" è stato scambiato per un video di al Qaeda a una riunione di comitato del Congresso. Oops.

<http://gamepolitics.livejournal.com/285129.html>

Ira Winkler sul perché lo spionaggio della NSA nuoce alla sicurezza:

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9000515> oppure <http://tinyurl.com/nkbam>

Come barare quando si scrivono elaborati scolastici:

<http://alex.halavais.net/?p=1427>

Anche voi potete spiare in Internet, proprio come la NSA.

<http://www.wired.com/news/technology/0,70914-0.html>

(E già che siamo in argomento, dovrete proprio leggere a proposito dell'attrezzatura che la NSA ha installato negli switch AT&T. Wow).

http://blog.wired.com/27BStroke6/att_klein_wired.pdf

Questo articolo sostiene che non v'è alcun modo di notificare una vulnerabilità informatica senza correre rischi. Qualsiasi cosa facciate, vi esponete a eventuali proseguiti legali.

<http://www.cerias.purdue.edu/weblogs/pmeunier/policies-law/post-38>

Robert Lemos su "Ethics and the Eric McCarthy Case" [L'etica e il caso McCarthy]

<http://www.robertlemos.com/2006/04/26/ethics-and-the-eric-mccarty-case/>

oppure <http://tinyurl.com/s8vvt>

Un Bill of Rights (Dichiarazione dei Diritti) per i robot:
<http://www.schneier.com/blog/archives/2006/05/a_robotic_bill.html>

TrueCrypt: crittografia istantanea con plausible deniability:
<<http://www.truecrypt.org/>>

Da Charlie Stross: "A report on the state of the National Identity Register, May 2016" [Un rapporto sullo stato del Registro d'Identità Nazionale, maggio 2016]. Si noti la data: si tratta di fiction.
<<http://www.antipope.org/charlie/blog-static/2006/05/17/#id-card-3>>

Eccellente citazione da Alexander Solzhenitsyn (1968) sulle informazioni e sulla privacy: "Durante la propria vita, ogni uomo riempie una serie di moduli destinati all'archiviazione, ognuno contenente una serie di domande... Vi sono quindi centinaia di piccoli fili che si dipartono da ogni uomo, milioni e milioni di fili in totale. Se tutti questi fili dovessero improvvisamente apparire, l'intera volta celeste sembrerebbe una grande ragnatela, e se si materializzassero in forma di nastri elastici, gli autobus, i tram, perfino le persone perderebbero la capacità di muoversi, e il vento non potrebbe trascinare frammenti di giornale o foglie d'autunno per le strade della città. Non sono visibili, non sono materiali, ma ogni uomo è continuamente consapevole dell'esistenza di quei fili... Ogni uomo, sempre consapevole dei propri fili invisibili, sviluppa naturalmente un certo rispetto per le persone che manipolano quei fili".

Nel lungo termine, le operazioni di data mining aziendale si rivelano essere un rischio maggiore per la privacy rispetto alle operazioni di data mining governativo. Ed ecco qui un prodotto IBM comunemente acquistabile:
<<http://www-306.ibm.com/common/ssi/fcgi-bin/ssialias?subtype=ca&infotype=an&appname=iSource&supplier=649&letternum=ENUSA06-0519>> oppure
<<http://tinyurl.com/q29er>>

L'Intelligence and Security Committee britannico ha pubblicato un rapporto sugli attentati terroristici del 7 luglio a Londra:
<http://www.cabinetoffice.gov.uk/publications/reports/intelligence/isc_7_july_report.pdf> oppure <<http://tinyurl.com/hazzn>>
Il governo britannico ha pubblicato una risposta:
<http://www.cabinetoffice.gov.uk/publications/reports/intelligence/govres_7july.pdf> oppure <<http://tinyurl.com/j8q5x>>
Informazioni sull'Intelligence and Security Committee:
<<http://www.cabinetoffice.gov.uk/intelligence/index.asp>>

Da un elenco di 100.000 password per un sito tedesco di incontri, si scopre che "123456" funziona l'1,4% delle volte, e che il 2,5% della totalità delle password inizia per "1234". Interessante.
<<http://www.heise.de/newsticker/meldung/73396>>

Una banca difende la propria scarsa sicurezza sostenendo che tutte le altre si comportano allo stesso modo.
<<http://blogs.zdnet.com/Ou/?p=226>>

Uno studio interessante riguardante la modalità con cui la legge europea tratterebbe la raccolta delle registrazioni telefoniche effettuate dalla NSA.
<http://www.concurringopinions.com/archives/2006/05/the_nsa_phone_c.html> oppure <<http://tinyurl.com/mpv6d>>

Una vignetta animata di satira politica sulle intercettazioni della NSA. E pure una canzone.
<<http://www.newsday.com/news/opinion/ny-wh-nsawiretapping,0,1906650.flas>>

h>

oppure <http://tinyurl.com/rg57v>>

È possibile seguire il corso "Welcome to Practical Aspects of Modern Cryptography" [Introduzione agli aspetti pratici della crittografia moderna] - a cura di Josh Benaloh, Brian LaMacchia e John Manferdelli. Università di Washington, Inverno 2006. I materiali del corso e i video delle lezioni sono online.

<http://www.cs.washington.edu/education/courses/csep590/06wi/>>

<http://www.cs.washington.edu/education/courses/csep590/06wi/lectures/>>

Un'affascinante intervista con un frodatore di carte di debito. Morale: proteggere questo sistema non sarà affatto semplice.

<http://smallworldpodcast.com/?p=391>>

E alcuni commenti da parte di un venditore di carte d'identità false, in caso pensavate che si potesse risolvere il problema ricorrendo a carte d'identità nazionali difficili da falsificare.

<http://www.cbsnews.com/stories/2006/06/02/ap/national/mainD8I07PHG0.shtml>> oppure <http://tinyurl.com/rafve>>

"How to Avoid Going to Jail under 18 U.S.C. Section 1001 for Lying to Government Agents" [Come evitare di finire in prigione per aver dichiarato il falso ad agenti governativi - legge 18 U.S.C. Section 1001]

<http://library.findlaw.com/2004/May/11/147945.html>>

Buon articolo che distingue fra i sensazionalismi e la realtà delle cose per quanto concerne la minaccia rappresentata da armi chimiche fatte in casa.

http://www.theregister.co.uk/2006/06/04/chemical_bioterror_analysis/>

Nascondete questo aggeggio nell'auto o nel bagaglio di qualcuno, o magari cucitelo al suo cappotto. Sarà poi possibile seguire ogni spostamento di questa persona tramite GPS. Occorre recuperare l'aggeggio per ottenere la riproduzione dei dati, ma presumibilmente la prossima generazione di tale dispositivo sarà interrogabile da remoto.

<http://www.thinkgeek.com/gadgets/security/8212/?cpg=cj>>

Il governo degli Stati Uniti sta richiedendo ai vari ISP di conservare i dati su di voi, in caso sia necessario avervi accesso.

<http://www.latimes.com/technology/la-fi-internet2jun02,0,622125.story?coll=la-home-headlines>> oppure <http://tinyurl.com/zpzzvz>>

Si noti che il Dipartimento di Giustizia ha menzionato due dei Quattro Cavalieri dell'Apocalisse di Internet: pedopornografi e terroristi. Se il Dipartimento riuscirà a trovare un modo per farci entrare anche i sequestratori e gli spacciatori di droga, molto probabilmente potrà fare ciò che vorrà.

Da "Assassination in the United States: An Operational Study of Recent Assassins, Attackers, and Near-Lethal Approachers" [L'Assassinio negli Stati Uniti: uno studio operativo sui recenti assassini, aggressori e potenziali killer] (un articolo del 1999 pubblicato nel "Journal of Forensic Sciences"): "Pochi aggressori o potenziali killer possedevano la destrezza e la spavalderia degli assassini di film o romanzi famosi. La realtà dell'assassinio negli Stati Uniti è molto più banale e mondana degli omicidi rappresentati sul grande schermo. Né mostri né martiri, i recenti assassini, aggressori e potenziali killer hanno mostrato schemi di pensiero e comportamentali anteriori al reato". La citazione è dall'ultima pagina; l'intero studio è una lettura molto interessante.

http://www.secretservice.gov/ntac/ntac_jfs.pdf>

Interessante articolo di giurisprudenza a cura di Helen Nissenbaum:

"Privacy as Contextual Integrity" [Privacy come integrità contestuale]
<<http://crypto.stanford.edu/portia/papers/RevnissenbaumDTP31.pdf>>

Nuove direzioni della guerra chimica: sostanze che rendono i soldati nemici sessualmente irresistibili fra loro, sostanze che attraggono sciame di vespe inferocite o che causano "una grave e continuata alitosi":

<<http://www.newscientist.com/article.ns?id=mg18524823.800>>
La tecnologia migliora sempre; non fa mai passi indietro. Vi sarà un tempo, forse in un futuro assai prossimo, in cui armi come queste esisteranno davvero.

Una vignetta sulla sorveglianza della NSA:
<<http://www.ibiblio.org/Dave/Dr-Fun/df200605/df20060517.jpg>>

Studio interessante sulla sicurezza delle smartcard senza contatto:
<<http://www.chi-publishing.com/samples/ISB0903HH.pdf>>

Rivelatore wireless di telecamere di sorveglianza:
<<http://www.brickhousesecurity.com/dd9000.html>>

Grande articolo che mette a confronto la barriera che Israele sta erigendo per proteggersi dalla Sponda Occidentale e la barriera ipotetica che gli Stati Uniti costruirebbero per proteggersi dal Messico: "Non c'è da stupirsi che la barriera [israeliana] sia considerata un'ottima cosa da parte di chi vive nella sua parte occidentale. Ma non sarà facile applicare questo modello alla frontiera USA-Messico. Per i cittadini statunitensi sarà arduo giustificare misure tanto drastiche quando il loro unico obiettivo è fermare l'immigrazione di chi cerca lavoro più che impedire eventuali tentativi di omicidio da parte degli immigrati. E i costi saranno il fattore più importante. È molto più facile aprire il portafoglio quando qualcuno minaccia di far saltare in aria un locale pubblico".
<<http://www.slate.com/id/2143104/>>

Una truffa VoIP da 1 milione di dollari:
<<http://www.networkingpipeline.com/news/188702745>>

Il NIST ha appena pubblicato "Recommendation for Random Number Generation Using Deterministic Random Bit Generators" [Indicazioni per la generazione casuale di numeri utilizzando generatori deterministici di bit casuali].
<<http://csrc.nist.gov/publications/nistpubs/index.html>>

La NSA sta passando al setaccio MySpace:
<<http://www.newscientisttech.com/article/mg19025556.200-pentagon-sets-it-s-sights-on-social-networking-websites.html>> oppure
<<http://tinyurl.com/fk3z6>>

** ** *

Inserirsi illecitamente nei computer tramite USB

Ho già trattato in precedenza dei rischi che comportano i piccoli dispositivi portatili; della quantità sempre maggiore di dati archiviabili in essi e la facilità con cui è possibile smarrirli. Ma vi è un altro rischio: se un aggressore riesce a convincervi di inserire il suo dispositivo USB nel vostro computer, ne può prendere il controllo. Da CSO Magazine:

"Si colleghi un iPod o una chiavetta USB a un PC Windows e il dispositivo esterno può letteralmente prendere il controllo della macchina e cercare documenti confidenziali, copiarli e nascondersi come file 'cancellati'. In alternativa, il dispositivo può semplicemente installare dello spyware o anche compromettere il sistema operativo. Due caratteristiche che rendono possibile tutto questo sono l'AutoRun di Windows, e il fatto che una periferica ha la capacità di servirsi di una cosa chiamata accesso diretto alla memoria (DMA). Il primo vettore di attacco è possibile e consigliabile disattivarlo, il secondo è il risultato di un errore di progettazione che probabilmente rimarrà con noi ancora a lungo".

Nell'articolo si entra nei dettagli, ma la sostanza è che si può configurare un file contenuto in un dispositivo USB in modo che si avvii automaticamente quando il dispositivo viene collegato a un computer. Quel file, naturalmente, può fare qualsiasi cosa si voglia che faccia.

Di recente ho notato una crescente letteratura riguardo a questo tipo di attacco. Il numero di Primavera 2006 di "2600 Magazine", per esempio, contiene un breve articolo intitolato "iPod Sneakiness" [iPod spione] (purtroppo non è reperibile online). L'autore fa notare come sia possibile chiedere innocentemente a qualcuno in un Internet Café il permesso di collegare il nostro iPod al suo computer per ricaricarlo: in questo modo è possibile rubargli password e file importanti.

Qualcuno ha utilizzato questo trucco in un test di penetrazione:

"Abbiamo pensato di provare qualcosa di diverso, adescando gli stessi dipendenti che erano in grande stato di allerta. Abbiamo raccolto tutte le chiavette USB senza valore (omaggi di vari produttori) collezionate in questi anni e vi abbiamo inserito il nostro software speciale. Ho detto a uno dei miei collaboratori di scrivere un Trojan che, quando eseguito dal computer dell'utente, raccogliesse password, informazioni di login e dati specifici della macchina, per poi inviarci queste informazioni via email.

"L'ostacolo seguente era riuscire a far arrivare le chiavette USB nelle mani degli utenti interni della cooperativa di credito. Sono entrato nella sede della cooperativa alle 6 del mattino per essere certo che nessun impiegato ci vedesse. Poi ho sistemato le chiavette nel parcheggio, nelle aree per fumatori, e in altre zone frequentate dagli impiegati.

"Una volta posizionate le chiavette USB, ho deciso di prendermi un caffè e osservare i dipendenti raggiungere il proprio posto di lavoro. Sorvegliare la struttura ha ripagato per tutto il tempo impiegato ad organizzare il test. Era davvero divertente osservare la reazione degli impiegati che trovavano una chiavetta USB. Era ovvio che l'avrebbero collegata al proprio computer non appena raggiunta la scrivania.

"Ho subito chiamato il mio collaboratore (l'autore del Trojan) per sapere se stesse ricevendo qualcosa. Lentamente ma inesorabilmente una serie di informazioni cominciava ad arrivare via email. Mi sarebbe piaciuto trovarmi all'interno dell'edificio e guardare gli impiegati connettere la chiavetta USB, togliere i vari file immagine da noi inseriti e avviare inconsapevolmente il nostro software".

Ci si può difendere in parte. Dal primo articolo:

"L'AutoRun è semplicemente una pessima idea. Chi inserisce CD-ROM o dispositivi USB nel proprio computer in genere vuole esaminare i contenuti del supporto, non certo avere programmi che partono in automatico. Fortunatamente è possibile disabilitare l'AutoRun. Un

approccio manuale molto semplice è quello di tenere premuto il tasto Maiuscolo all'inserimento di un CD o di un dispositivo USB. Un metodo migliore è quello di eliminare completamente la funzione modificando il Registro di Windows. In rete vi sono svariate istruzioni per procedere (basta cercare 'disable autorun'), oppure si può scaricare e utilizzare il programma Microsoft TweakUI, che fa parte della suite Windows XP PowerToys. Con Windows XP è anche possibile disattivare l'AutoRun dei CD facendo clic con il pulsante destro del mouse sull'icona del lettore CD nell'explorer di Windows: si seleziona AutoPlay e quindi si sceglie 'Take no action' per ogni tipo di unità disco elencata. Purtroppo la disattivazione dell'AutoPlay per i CD non sempre porterà alla disattivazione dell'AutoPlay per i dispositivi USB, pertanto la modifica al registro è il modo più sicuro di procedere".

Negli anni Novanta il sistema operativo Macintosh possedeva questa funzionalità, ma fu rimossa dopo che un virus ne fece uso nel 1998. Anche Microsoft deve togliere questa funzionalità.

Ma è soltanto una difesa parziale. Nel test di penetrazione non hanno utilizzato l'AutoRun. Hanno semplicemente creato un file abbastanza accattivante: sono state le persone che hanno trovato le chiavette USB a invocare manualmente l'eseguibile.

<http://www.csoonline.com/read/050106/ipods.html>
http://www.darkreading.com/document.asp?doc_id=95556&WT.svl=column1_1
http://www.darkreading.com/boards/message.asp?msg_id=134658

Il mio precedente intervento:

http://www.schneier.com/blog/archives/2005/07/risks_of_losing.html

** **

Il Canile: KRYPTO 2.0

Questo sito Web è buffissimo:

"Prove della sicurezza di Krypto! Quale sarebbe, se uno provasse uno dei file codificati Krypto non autorizzato per decodificare. Un file codificato con la lunghezza di 18033 indicazioni ha quindi secondo il calcolo, 256 bit altamente 18033 indicazioni = 6,1843558143632013533192271736305e+43427 possibilità del file. Ogni possibilità del file ha esattamente 18033 indicazioni e/o byte. Moltiplicato dal numero di possibilità del file allora avere bisogno dei risultati nella memoria. Quelli sono allora: 1,1152248840041161000440562362208e+43432 byte. Quelli sono allora: quantità di dati di byte di 1,0386341102459617890827881509632e+43423 Giga. Quello è un numero con 43424 posti. Posso certamente effettuare tanto posto di memoria dato esso nel mondo intero non e/o mai. Ed il problema capo ora è, che ora è il file correttamente decodificato. Chi non conosce può dire soltanto là. Quello non sa così esattamente! Possono codificare naturalmente naturalmente anche ancora successivamente parecchie volte, anche fino all'infinità".

Traduzione automatica della versione inglese presente sul sito, che a sua volta è una traduzione automatica dell'originale tedesco. Mi viene il mal di testa solo cercando di leggerla.

<http://kryptochef.net/index2e.htm>

** **

al cliente non importa di ricevere o no uno scontrino.

Perciò ecco che cosa fa il proprietario del negozio: "assume" il cliente. Mettendo un cartello che dice "Il vostro acquisto è gratis se non ricevete lo scontrino", il proprietario fa in modo che sia il cliente a sorvegliare l'impiegato. Il cliente si assicura che l'impiegato gli rilasci uno scontrino, e di conseguenza si riduce la possibilità di furto.

Vi è una regola generale nell'ambito della sicurezza per allineare l'interesse con la possibilità. Il cliente ha la possibilità, la facoltà di osservare l'impiegato: il cartello fornisce al cliente un interesse, un incentivo per farlo.

In "Beyond Fear" ho parlato delle truffe dei bancomat: si può vedere in azione lo stesso meccanismo:

"Quando i possessori di bancomat negli Stati Uniti si sono lamentati di prelievi fantasma nei loro conti correnti, i tribunali solitamente stabilivano che le banche dovevano provare la frode. Conseguentemente, era nell'interesse delle banche migliorare la sicurezza e mantenere il tasso di frode a livelli minimi, perché erano le banche a pagare i costi delle frodi. Nel Regno Unito accadeva l'opposto: i tribunali si schieravano in genere con le banche e assumevano che ogni tentativo di rigettare tali prelievi fosse una frode perpetrata dal correntista, e il correntista doveva provare la sua innocenza. Questo ha fatto sì che le banche avessero priorità diametralmente opposte: non importava migliorare la sicurezza perché a loro stava bene scaricare i problemi sui correntisti e incriminarli in caso di lamentele. Risultato: negli Stati Uniti le banche hanno migliorato la sicurezza degli sportelli bancomat per prevenire ulteriori perdite (la maggior parte dei casi di frode, infatti, non erano dovuti a mancanze del cliente), mentre nel Regno Unito le banche non hanno fatto nulla di concreto".

Le banche hanno avuto la possibilità di migliorare la sicurezza. Negli Stati Uniti avevano anche l'interesse a farlo, ma nel Regno Unito solo il correntista ne aveva l'interesse. Per vedere un miglioramento della sicurezza degli sportelli bancomat si è dovuto aspettare che i tribunali britannici facessero marcia indietro e allineassero l'interesse con la possibilità.

La sicurezza informatica non è diversa. Per anni sono stato a favore delle responsabilità per il software prodotto. I produttori di software si trovano nella posizione migliore per migliorare la sicurezza del software: ne hanno la possibilità. Sfortunatamente, però, non hanno molto interesse a farlo. Le funzionalità, i tempi di produzione e la redditività sono molto più importanti. Le responsabilità sul software cambieranno tutto questo, allineando l'interesse con la possibilità, e aumentando la sicurezza del software.

Un'ultima storia. In Italia, frodare le tasse è stato per molto tempo un hobby nazionale (forse lo è ancora, non so). Il governo, stanco di esercizi commerciali che non registravano correttamente le vendite e che quindi non pagavano le tasse, approvò una legge che regolava i clienti. Ogni cliente che avesse acquistato qualcosa in un negozio e che fosse stato fermato entro una certa distanza dal negozio stesso, avrebbe dovuto mostrare lo scontrino, altrimenti sarebbe incorso in una multa. Proprio come nella vicenda "Il vostro acquisto è gratis se non ricevete lo scontrino", la legge trasformò i clienti in ispettori fiscali. I clienti ovviamente obbligavano i commercianti a produrre uno scontrino, e quindi un tracciato di verifica cartaceo per ogni acquisto, costringendo i commercianti a pagare le tasse richieste.

Fu un'ottima idea, ma non funzionò molto bene. Ai clienti, specialmente ai turisti, non piaceva essere fermati dalla polizia. Hanno quindi iniziato a richiedere alle forze dell'ordine di provare che il tale oggetto fosse stato effettivamente appena acquistato. Minacciare le persone con multe e sanzioni in caso non sorvegliassero i commercianti non si è rivelato un incentivo efficace come quello di offrire ai clienti un premio (l'acquisto gratis) in caso di mancato scontrino.

L'interesse deve sempre allinearsi con la possibilità, ma occorre fare attenzione a come generare tale interesse.

Questo articolo è originariamente apparso su Wired.com.

<http://www.wired.com/news/columns/0,71032-0.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.

Inoltre 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.

Crypto-Gram è una newsletter personale. Le opinioni qui espresse non sono necessariamente quelle di Counterpane Internet Security, Inc.

Copyright (c) 2006 by Bruce Schneier.