

CRYPTO-GRAM
15 giugno 2005

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

Edizione italiana curata da Communication Valley SpA

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

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

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

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

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

In questo numero:

Attacchi in Internet nel 2005: andamenti e tendenze
Degli stupidi acquistano biglietti per un concerto falsificati
Tecnologia raggi X a retrodiffusione
Le ristampe di Crypto-Gram
Attacchi dall'interno
L'accuratezza dei Data Broker commerciali
News
Eric Schmidt sulla Segretezza e la Sicurezza
Ridotta all'osso la legge sulla privacy sanitaria statunitense
I rischi dei cellulari sugli aerei
Miliardi sprecati in sicurezza antiterrorismo
Le News di Counterpane
Un attacco alla procedura di pairing del protocollo Bluetooth
Password Safe 2.11
La pubblica divulgazione della perdita dei dati personali
Prendere in ostaggio i file di un computer
Un'altra minaccia all'antrace si rivela un falso allarme
Commenti dei lettori

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

Attacchi in Internet nel 2005: andamenti e tendenze

Counterpane Internet Security, Inc. effettua il monitoraggio di più di 450 reti in 35 paesi, in qualsiasi fuso orario. Nel 2004 abbiamo visto 523 miliardi di eventi network e i nostri analisti hanno investigato 648.000 "ticket" di sicurezza. Quella che segue è una panoramica di ciò che sta succedendo in Internet oggi, e di ciò che ci aspettiamo possa accadere nei prossimi mesi.

Nel 2004, il 41% degli attacchi che abbiamo rilevato si trattava di attività non autorizzate di vario genere, il 21% erano scanning, il 26% erano accessi non autorizzati, il 9% erano DoS (Denial of Service), e il 3% erano abusi di applicazioni.

Nei mesi scorsi, i due vettori di attacco che abbiamo notato in quantità sono stati a danno dell'interfaccia Windows DCOM (Distributed Component Object Model) del servizio RPC (Remote Procedure Call) e contro il servizio Windows LSASS (Local Security Authority Subsystem Service). Questi sembrano essere il bersaglio preferito degli autori di worm e virus, e ci aspettiamo che questa tendenza continui.

Il trend dei virus non promette nulla di buono. Negli ultimi sei mesi del 2004, abbiamo notato una moltitudine di attacchi basati su vulnerabilità dei browser (come la vulnerabilità del formato grafico GDI-JPEG e IFRAME) e un aumento di sofisticati attacchi basati su worm e virus. Più di 1000 nuovi worm e virus sono stati scoperti negli ultimi sei mesi.

Nel 2005 ci aspettiamo di assistere a worm e virus ancora più complessi che incorporano un comportamento complesso: worm polimorfi, worm metamorfici, e worm che fanno uso dell'occultamento dell'entry-point. Per esempio, SpyBot.KEG è un sofisticato worm di verifica delle vulnerabilità che rimanda all'autore del worm attraverso canali IRC un resoconto delle vulnerabilità scoperte.

Ci aspettiamo di vedere minacce miste: codice di exploit che combina codice malevolo e vulnerabilità così da lanciare un attacco. Ci aspettiamo che il server Web Microsoft IIS (Internet Information Services) continui ad essere un bersaglio attraente. Tuttavia, con il passaggio a Windows 2003 e a IIS 6 da parte di un numero sempre maggiore di aziende, ci aspettiamo una diminuzione degli attacchi contro IIS.

Aspettiamo inoltre di vedere il networking peer-to-peer come vettore per il lancio di altri virus.

Un'altra tendenza che stiamo incominciando a vedere, poi, sono i worm mirati. Di recente vi sono stati worm che hanno utilizzato tecniche di terze parti per la raccolta informazioni, come Google, per una forma di ricognizione avanzata. Questo porta a una metodologia di propagazione intelligente; invece di propagarsi in maniera sparpagliata, questi worm si stanno concentrando su bersagli precisi. Identificando i bersagli tramite un sistema di terze parti di raccolta dati, i worm riducono il rumore che farebbero normalmente scegliendo bersagli a caso, aumentando così la finestra di opportunità nell'intervallo temporale che va dal rilascio al primo rilevamento.

Un altro trend del 2004 che ci aspettiamo continui anche nel 2005 è il crimine. L'attività di hacking, da ricerca hobbistica a scopo di notorietà è diventata ricerca criminale a scopo di guadagno. Gli hacker possono vendere vulnerabilità sconosciute (dette "zero-day exploit") sul mercato nero, a criminali che le useranno per penetrare in altri computer. Gli hacker che possiedono reti di macchine violate possono far soldi vendendole a spammer o a phisher. Possono utilizzarle per attaccare altre reti. Abbiamo iniziato a vedere estorsioni criminali su Internet: hacker con reti di macchine violate che minacciano di lanciare attacchi DoS ai danni di aziende. La maggioranza di questi attacchi sono contro società marginali (scommesse online, giochi online, pornografia) e contro reti all'estero. Più queste estorsioni hanno successo, più i criminali saranno incoraggiati.

Ci aspettiamo di vedere un aumento degli attacchi ai danni di istituzioni finanziarie, dato che i criminali cercano nuovi sistemi per commettere frodi. Ci aspettiamo anche di vedere un aumento degli attacchi dall'interno a scopi di profitto criminale. Già la maggior parte degli attacchi mirati, contrariamente agli attacchi di opportunità, ha origine da dentro la rete dell'azienda sotto attacco.

Ci aspettiamo inoltre di vedere un aumento di hacking politicamente motivato che colpisca indifferentemente paesi, aziende in industrie "politiche" (petrolchimica, farmaceutici, ecc.), organizzazioni politiche. Anche se non ci aspettiamo di vedere atti terroristici in Internet, ci aspettiamo di vedere un maggior numero di attacchi di disturbo da parte di hacker con motivazioni politiche.

Internet è sempre un luogo pericoloso, ma non ne prevediamo un abbandono da parte di persone e aziende. Le ragioni economiche e sociali per usare Internet sono ancora troppo impellenti.

Questo articolo è stato originariamente pubblicato nel numero del 5 giugno di Queue.
<<http://www.schneier.com/essay-085.pdf>>

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

Degli stupidi acquistano biglietti per un concerto falsificati

A un concerto rock a Boston, centinaia di persone hanno comprato biglietti fasulli dai bagarini - alcuni pagando addirittura 2000 dollari per averli. Probabilmente penserete a chissà quale fantasioso sistema di contraffazione: niente del genere. I biglietti erano stampe comprate da bagarini online.

I biglietti online sono una gran comodità. Ogni biglietto è provvisto di un codice a barre unico. Ne potete stampare finché volete, ma gli scanner all'ingresso del concerto accetteranno ogni codice a barre una sola volta.

Soltanto un idiota comprerebbe una stampa da un bagarino, perché non c'è modo di verificare che il biglietto sia venduto una sola volta. Questo forse è ovvio per i lettori di questa newsletter, ma pare che non sia proprio ovvio per tutti.

Trovo tutto ciò decisamente affascinante. La verifica online di token di autenticazione dovrebbe rendere più difficile eventuali falsificazioni, perché assume che il token "fisico" possa essere copiato. Funziona di sicuro per il management: anche se un falsario produce delle copie, solo una persona per ogni posto viene ammessa nel luogo del concerto. Ma evidentemente non per il pubblico, almeno finché non capirà come funziona il sistema.

<http://sport.monstersandcritics.com/news/article_1002583.php/Boston_U2_fans_stung_with_fake_tickets> oppure <<http://tinyurl.com/9fzag>>
<<http://www.u2tours.com/news/article.src?ID=1023>>

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

Tecnologia raggi X a retrodiffusione

La tecnologia raggi X a retrodiffusione è un modo di utilizzare i raggi X per vedere all'interno di oggetti. I dettagli scientifici sono un po' complicati, ma il risultato è la possibilità di vedere le persone nude. La TSA ha di recente annunciato una proposta per adottare queste macchine per lo screening dei passeggeri delle linee aeree.

Questo compromesso di sicurezza mi piace poco. Certo, queste macchine a raggi X a retrodiffusione potrebbero rilevare cose che sfuggono a un normale controllo. Ma già penso che si stiano spendendo troppe energie nel controllare i passeggeri a scapito di controllare il bagaglio e gli impiegati dell'aeroporto... per non dire nulla del denaro che dovremmo spendere sulla sicurezza in generale, non limitata agli aeroporti.

Inoltre, queste macchine sono costose e la tecnologia incredibilmente intrusiva. Non credo che le persone dovrebbero essere costrette a fare lo spogliarello prima di imbarcarsi su un aereo. E credo che la maggior parte delle persone sarebbe inorridita dalla prospettiva di essere vista nuda dagli agenti di sicurezza.

Penso che vi sarà un'ondata di opposizione popolare a questa idea. A parte i soliti gruppi a favore della privacy e delle libertà civili, mi aspetto l'indignazione dei gruppi di fondamentalisti cristiani

nei confronti di questa tecnologia. Forse potremmo trovare un gruppo di top model che parli contro l'invasione di questo genere di controlli.

<<http://www.epic.org/privacy/airtravel/backscatter/default.html>>
<<http://www.epic.org/privacy/surveillance/spotlight/0605.html>>

La notizia:

<http://news.com.com/Airport+screeners+could+see+X-rated+X-rays/2100-7348_3-5718163.html> oppure <<http://tinyurl.com/caus8>>

** **

Le ristampe di Crypto-Gram

Crypto-Gram è attualmente al suo ottavo anno di pubblicazione. I numeri precedenti coprono tutta una serie di argomenti legati alla sicurezza e si possono trovare a questo indirizzo: <<http://www.schneier.com/crypto-gram.html>>. Quella che segue è una selezione di articoli apparsi in questo mese gli anni scorsi (le traduzioni in italiano degli articoli sott'indicati possono essere reperite all'indirizzo <http://www.cryptogram.it>, ndt).

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 crittosistemi:

<<http://www.schneier.com/crypto-gram-9806.html#side>>

** **

Attacchi dall'interno

Il CERT ha pubblicato uno studio sulle minacce provenienti dall'interno. Ha analizzato 49 attacchi dall'interno compiuti fra il 1996 e il 2002 e ha tracciato alcune conclusioni sugli attacchi e gli aggressori. Nulla invece per quanto riguarda la prevalenza e soprattutto i dettagli, i particolari di questi attacchi.

Il resoconto è piuttosto ovvio e non merita più di una scorsa. Ma la particolare metodologia racconta solo una parte della storia.

Siccome lo studio è incentrato in special modo sugli attacchi dall'interno ai danni di sistemi di informazioni, più che su attacchi che si servono di sistemi di informazioni, esso tratta primariamente atti distruttivi. Naturalmente il movente principale è la vendetta nei confronti del datore di lavoro.

A quanto mi è dato vedere, il rapporto non parla di quegli attacchi che si servono di sistemi di informazioni per avvantaggiare l'aggressore in altri modi. Questi attacchi comprenderebbero l'appropriazione indebita -- che, a naso, è molto più comune della vendetta.

Un altro elemento che il rapporto non sembra riconoscere è il fatto che i ricercatori stiano solo esaminando gli attacchi scoperti. Non mi stupisce che molti degli aggressori siano stati presi, visto che i loro attacchi hanno attirato attenzione. E questo non fa che consolidare il medesimo (pre)concetto: che la violazione di una rete è molto più visibile del furto.

Si tratta di attacchi preoccupanti, ma io sarei ancor più preoccupato di attacchi dall'interno che non sono altrettanto evidenti.

Ad ogni modo vi sono alcune statistiche interessanti su coloro i quali usano sistemi di informazioni per vendicarsi dei propri datori di lavoro. Nel 62% dei casi "un evento lavorativo negativo ha innescato molte delle azioni dell'aggressore interno". Nell'82% dei casi, chi ha violato l'azienda dove lavorava "ha mostrato un comportamento anomalo sul lavoro prima di mettere in pratica le proprie azioni". L'84% degli attacchi erano motivati dal desiderio di vendetta, e l'85% degli aggressori aveva documentati motivi di lagnanza nei confronti del datore di lavoro o di un collega. Il 96% degli aggressori sono di sesso maschile, e il 30% era stato precedentemente arrestato. Il 18% era stato arrestato per aggressioni violente, l'11% per aggressioni legate a droga o alcol, e l'11% per furti non legati a frodi finanziarie.

<http://blogs.washingtonpost.com/securityfix/2005/05/employees_takin.html>
<<http://tinyurl.com/72v7p>>

oppure

Lo studio:

<http://www.secretservice.gov/ntac/its_report_050516.pdf>

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

L'accuratezza dei Data Broker commerciali

PrivacyActivism ha rilasciato uno studio su ChoicePoint e Acxiom, due dei maggiori Data Broker statunitensi. Lo studio esamina l'accuratezza delle informazioni e la risposta alle richieste di resoconti.

Niente di buono.

Dal comunicato stampa: "Il 100% degli undici partecipanti allo studio ha scoperto errori nei background check forniti da ChoicePoint. La maggior parte dei partecipanti ha trovato errori

Un altro furto di informazioni. Non si tratta di una perdita, ma di un furto perpetrato da un'organizzazione criminale. Ed è stato anche un attacco molto low-tech: "I sospettati hanno raccolto i dati sui conti correnti mentre lavoravano in banca, poi hanno stampato le informazioni che apparivano a video oppure le hanno trascritte a mano -- ha dichiarato Lomia. Le informazioni sono state poi passate a una società chiamata DRL Associates Inc., che è stata creata come copertura per le operazioni. DRL si pubblicizzava come servizio di localizzazione degli emarginati e come agenzia di esazione, ma non era stata debitamente autorizzata dallo stato per svolgere tali attività -- hanno dichiarato le forze dell'ordine".

<<http://www.computerworld.com/securitytopics/security/cybercrime/story/0,10801,101903,00.html>> oppure <<http://tinyurl.com/avsqq>>

David Card ed Enrico Moretti, entrambi economisti all'UC Berkeley, hanno pubblicato un'analisi interessante sulle macchine per il voto elettronico e le elezioni 2004: "Does Voting Technology Affect Election Outcomes?

Touch-screen Voting and the 2004 Presidential Election" [La Tecnologia per il Voto può influenzare i Risultati Elettorali? Le Votazioni con Sistema Touch-Screen e le Elezioni Presidenziali 2004].

<<http://emlab.berkeley.edu/~moretti/dre.pdf>>

Una corte d'appello in Minnesota ha stabilito che la presenza di software crittografico su un computer può essere considerata come prova di intenzioni criminose.

<http://news.com.com/Minnesota+court+takes+dim+view+of+encryption/2100-1030_3-5718978.html> oppure <<http://tinyurl.com/ae9j4>>

Il testo dell'ordinanza:

<<http://www.lawlibrary.state.mn.us/archive/ctappub/0505/opa040381-0503.htm>>

oppure

<<http://tinyurl.com/b6wwj>>

Il commento intelligente di Jennifer Granick:

<http://www.granick.com/archive/2005_05_01_theshout_archive.html#111758156022936540>

oppure <<http://tinyurl.com/8zfbg>>

Un'analisi del worm Witty. Fra le altre cose, i ricercatori hanno trovato il punto iniziale dell'infezione (paziente 0). Essi ritengono inoltre che l'attacco si trattava, almeno in parte, di un deliberato attacco cibernetico ai danni dell'Esercito degli Stati Uniti; una base militare è stata presa volontariamente di mira nella hotlist del worm. E sospettano che il worm sia stato scritto da qualcuno che lavora all'interno del produttore di sistemi di intrusion detection ISS.

<<http://www.cc.gatech.edu/~akumar/witty.html>>

Un importante caso di spionaggio informatico sta facendo notizia in Israele. "Fra le aziende sospettate di aver commissionato lo spionaggio (che è stato messo in opera immettendo dei Trojan horses nei computer della concorrenza) c'è la compagnia televisiva satellitare Yes, che è sospettata di aver spiato ai danni della compagnia televisiva via cavo HOT; le aziende di telefonia cellulare Pelephone e Cellcom, sospettate di aver spiato la loro rivale Partner e Mayer, importatore per l'Israele di Volvo e Honda, sospettato di aver spiato Champion Motors, importatore di Audi e Volkswagen. Programmi di spionaggio sono stati anche introdotti nei computer di grandi compagnie come Strauss-Elite, Shekem Electric e il quotidiano di affari e finanza Globes".

<<http://arik.baratz.org/wordpress/2005-05-29/trojan-horses-abound/>>

<<http://www.cnn.com/2005/TECH/06/01/israel.computer.breakin.ap/>>

<<http://www.jpost.com/servlet/Satellite?pagename=JPost/JPArticle/ShowFull&cid=1117333096614>> oppure <<http://tinyurl.com/8ucqc>>

Errori di ortografia inseriti volontariamente nelle carte d'identità del Belgio, come misura preventiva anti-contraffazione:

<http://news.com.com/2061-10786_3-5719227.html>

<http://www.theregister.co.uk/2005/05/26/belgian_id_card_plan/>

Sensori a radiofrequenze camuffati da rocce e usati in ambito militare:

<<http://www.webwarrior.net/print.php?sid=6502>>

Si discute su questo genere di cose da un pezzo. Uno dei migliori interventi è ancora quello di Martin Libicki risalente alla metà degli anni Novanta: "The Mesh and the Net: Speculations on

Armed Conflict in a Time of Free Silicon" [La maglia e la rete: riflessioni sui conflitti armati nell'era del silicone libero].

<<http://www.amazon.com/exec/obidos/tg/detail/-/016061161X/002-7699408-6685612>> oppure
<<http://tinyurl.com/d6lfd>>
<<http://www.ndu.edu/inss/McNair/mcnair28/m028ch00.html>>

Trovo che le misure di sicurezza che Mark Felt ha richiesto a Bob Woodward siano affascinanti.

<http://www.washingtonpost.com/wp-dyn/content/article/2005/06/01/AR2005060102124_pf.html>

La moneta corrente in Sudan viene stampata su carta normale, con una qualità cromatica e d'immagine scarsa e poco coerente, e non ha nessuna caratteristica anti-contraffazione, nemmeno dei numeri di serie. Come mai la sicurezza funziona, allora? Perché chiunque falsifichi banconote verrà messo di fronte a un plotone d'esecuzione e fucilato.

<<http://www.npr.org/templates/story/story.php?storyId=4673945>>

Impressionante abuso di potere da parte della TSA:

<<http://www.komotv.com/stories/37150.htm>>

In gennaio ho parlato dei nuovi documenti d'identità biometriche del Dipartimento per la Sicurezza Nazionale:

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

In aprile ho fatto riferimento a un'analisi del documento d'identità fatta da EPIC:

<<http://www.epic.org/privacy/surveillance/spotlight/0405.html>>

In maggio, Phil Libin ha scritto un commento con molte inesattezze a riguardo dell'analisi dell'EPIC su CNet:

<<http://news.com.com/2010-7348-5710529.html>>

Abbiamo scritto una risposta:

<<http://www.epic.org/privacy/surveillance/spotlight/0405response.html>>

E Libin ha risposto alla nostra risposta:

<http://www.vastlyimportant.com/vastly/2005/05/epic_responds.html>

Due ricercatori dell'Institute for Cryptology and IT-Security hanno generato file PostScript con identiche somme MD5 ma dai contenuti completamente differenti (e sensati!):

<<http://www.cits.rub.de/MD5Collisions/>>

Altri attacchi MD5:

<http://www.schneier.com/blog/archives/2005/03/more_hash_funct.html>

Chiusure di sicurezza per vaschette di gelato:

<<http://store.benjerry.com/pintlock.html>>

<http://www.dougydoug.com/if_nothing_else.htm>

Un affascinante articolo di una pubblicazione di giurisprudenza sulla definizione dell'accesso nel cyberspazio:

<http://papers.ssrn.com/sol3/papers.cfm?abstract_id=399740>

Un sistema di sicurezza della Torah che si conforma alla legge giudaica:

<http://wirednews.com/news/culture/0,1284,67743-2,00.html?tw=wn_story_page_next1>

oppure <<http://tinyurl.com/acl9g>>

I fisici spesso utilizzano "137" come codice per chiudere le loro valigette. "La costante di struttura è stata calcolata essere 1//137.03599976, arrotondata a 1/137: di qui il numero 137 ha assunto fama leggendaria presso i fisici (in genere è la combinazione per aprire le loro ventiquattrore)".

<<http://www.sciam.com/article.cfm?chanID=sa006&articleID=0005BFE6-2965-128A-A96583414B7F0000&pageNumber=2&catID=2>> oppure <<http://tinyurl.com/cqt6r>>

Il nuovo Pentium D incorporerà della tecnologia che potrà essere usata per supportare il DRM.

<<http://www.digitmag.co.uk/news/index.cfm?NewsID=4915>>

Negli Stati Uniti, la privacy sanitaria è in larga parte regolata da una legge del 1996 chiamata HIPAA. Fra i molti provvedimenti, la HIPAA regola la privacy e la sicurezza che circonda gli archivi medici elettronici. La HIPAA specifica le sanzioni civili a cui vanno incontro le compagnie che non si attengono alle disposizioni, e le sanzioni penali a cui sono soggetti singoli individui e società che sottraggono o abusano volontariamente dei dati dei pazienti.

L'industria della sanità ha sempre considerato irrilevanti le sanzioni civili. Ora quelle penali sono state ridotte all'osso. Il Dipartimento di Giustizia ha stabilito che le sanzioni penali debbano essere applicate ad assicuratori, medici, ospedali e altri fornitori di servizi, ma non necessariamente ai loro impiegati o ad esterni che rubano dati medici personali. Questo significa che se un impiegato fa un uso improprio di dati sensibili, a meno che non sia stato il suo capo a dirgli di farlo, non potrà essere perseguito secondo la HIPAA. E il fornitore non può essere perseguito a meno che non si tratti di politica organizzativa ufficiale.

È una questione complicata. Peter Swire ha lavorato molto estesamente a questa legge in qualità di Chief Counselor for Privacy della Presidenza, e io lo citerò in maniera altrettanto estesa. Per cominciare, la storia di un tizio che è stato condannato secondo la parte penale di questo statuto.

“Nel 2004 il Procuratore di Stato in Seattle annunciò che Richard Gibson era stato formalmente accusato di violazione della legge HIPAA sulla privacy. Gibson era flebotomista e assistente di laboratorio in un ospedale. Durante il lavoro ha consultato gli archivi clinici di una persona affetta da un cancro terminale. Gibson ha quindi ottenuto carte di credito a nome del paziente e ha superato i 9.000 dollari di addebiti, in special modo per acquistare videogiochi. In una dichiarazione alla corte, il paziente ha sostenuto di avere 'perso un anno di vita, fisicamente e mentalmente per sopportare lo stress' di aver a che fare con agenzie di recupero crediti e altri effetti delle azioni di Gibson. Gibson ha firmato un patteggiamento ed è stato condannato a 16 mesi di prigione”.

Secondo l'attuale Dipartimento di Giustizia in carica, Gibson è stato condannato per errore. Presumo che il suo legale ci stia lavorando su, e mi auguro che si possa avere un secondo processo per reato di furto di identità. Ma dato che Gibson (o altri come lui) stava agendo nell'esercizio delle proprie funzioni, non può essere perseguito secondo la HIPAA. E dato che Gibson (o altri come lui) stava facendo qualcosa di non autorizzato dal suo datore di lavoro, l'ospedale non può essere perseguito secondo la HIPAA.

L'industria della sanità si è opposta alla HIPAA fin dal principio, perché impone limiti ai suoi affari in nome della sicurezza e della privacy. Questa ordinanza è il prodotto di intense pressioni politiche da parte dell'industria presso il Department of Health and Human Services e il Dipartimento di Giustizia, ed è il risultato di una richiesta di opinione da parte del HHS.

Secondo l'analisi di Swire, il Dipartimento di Giustizia in carica: “Per essere un professore di legge che insegna interpretazione statutaria, l'opinione dell'ufficio legale (OLC) è terribilmente frustrante da leggersi. Sembra un verbalino di una sola delle due parti di una disputa. Peggio, sembra un verbale che sa di difendere la parte perdente ma deve comunque uscirsene con una risposta predeterminata”.

Io ho preso parte alla mia ragione di conferenze HIPAA sulla sicurezza. Fino al punto in cui la Sanità sta seguendo la legge HIPAA (e in larga misura sta aspettando di vedere come sarà fatta rispettare) lo sta facendo a causa delle sanzioni penali. Sa che le sanzioni civili non sono così gravi, e che sono un costo che deriva dal fare business. Ma le sanzioni penali c'erano ed erano una minaccia. Ora che non ci sono più, la pressione sull'industria della sanità affinché protegga la privacy dei pazienti è enormemente diminuita.

Ancora Swire: “La spiegazione più semplice del parere negativo dell'ufficio legale (OLC) è la politica. Parti dell'industria della sanità hanno fatto dure pressioni politiche affinché la HIPAA fosse abrogata nel 2001. Quando il Presidente Bush ha deciso di mantenere la regolamentazione

sulla privacy (molto probabilmente lo ha deciso in base al suo sincero punto di vista personale in materia), gli sforzi dell'industria hanno cambiato direzione. La pressione dell'industria ha impedito all'HHS di tirar fuori una sola causa civile dalle 13.000 citazioni in giudizio. Ora, dopo che un Procuratore di Stato ha avuto l'iniziativa di perseguire Gibson, gli alti funzionari a Washington hanno posto un freno alle sanzioni penali. La partecipazione di alti funzionari politici nell'interpretazione di uno statuto, invece di essersi affidati a legali d'ufficio, rende ancor più convincente il movente politico che sta dietro a questa mossa”.

Questo genere di cose è ancor più grande della sicurezza dei dati medici dei cittadini americani. La nostra Amministrazione sta cercando di raccogliere sempre più dati nel tentativo di combattere il terrorismo. Parte di questo tentativo è convincere sia gli americani sia gli stranieri, che questi dati verranno protetti. Quando riduciamo le protezioni sulla privacy perché potrebbero ostacolare il business, stiamo dicendo al mondo che la privacy non è uno dei nostri interessi primari.

Se l'Amministrazione non crede che dobbiamo attenerci alle leggi che regolamentano la privacy dei dati medici, che cosa vi fa pensare che essi stiano attenendosi alle leggi che regolamentano il FISA?

La notizia:

<<http://www.nytimes.com/2005/06/07/politics/07privacy.html>>

L'articolo di Swire:

<<http://www.americanprogress.org/site/pp.asp?c=biJRJ8OVF&b=743281>>

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

I rischi dei cellulari sugli aerei

Tutti, tranne chi ama la pace e la quiete, pensano che sia una buona idea permettere l'uso di telefoni cellulari sugli aerei, e stanno ragionando sui dettagli tecnici. Ma il Governo degli Stati Uniti è preoccupato che i terroristi possano fare telefonate dagli aerei, coordinandosi con dei complici a terra, su un altro volo, o anche seduti altrove sullo stesso volo. Oppure che possano sfruttare la tecnologia per innescare a distanza un esplosivo posto sull'aereo.

Tutto questo va ben oltre l'idiozia. Ancora una volta eccoci di fonte all'argomento secondo cui una particolare tecnologia possa venire usata per atti criminosi, per cui bisogna proibirla o controllarla. Il problema è che quando si proibisce o si controlla una tecnologia, ci si priva anche delle funzioni positive della tecnologia stessa. La sicurezza è sempre un compromesso. Quasi tutte le tecnologie possono essere usate in maniera positiva e in maniera negativa; in "Beyond Fear" le chiamo "dual use technologies" [tecnologie a doppio uso]. Nella maggior parte dei casi, gli utilizzi positivi sono di gran lunga maggiori di quelli negativi, e siamo una società migliore se abbracciamo gli utilizzi positivi e troviamo qualche altro modo per occuparci di quelli negativi.

Non proibiamo le automobili perché i rapinatori di banche potrebbero usarle per fuggire più rapidamente. Non proibiamo i cellulari perché gli spacciatori di droga li utilizzano per organizzare le vendite. Non proibiamo il denaro perché i rapitori lo usano. Infine non proibiamo la crittografia perché i "cattivi" la usano per tenere segrete le loro comunicazioni. In tutti questi casi i benefici che ricava la società dalla presenza di una data tecnologia sono molto maggiori dei benefici che la società avrebbe controllando, limitando o vietando la tecnologia.

Le misure di sicurezza che obbligano gli aggressori a fare piccole modifiche ai loro piani non sono degli ottimi compromessi. Proibire i telefoni cellulari sugli aerei ha senso soltanto se i terroristi stanno pianificando di utilizzarli sugli aerei e abbandoneranno i loro propositi di attacco semplicemente perché non possono sferrarlo. Se il loro piano non prevede comunicazioni aria-

terra, o se non prevede affatto un volo, allora la misura di sicurezza è uno spreco. E, ancora peggio, così facendo ci siamo privati di tutti gli usi positivi di quella tecnologia.

<<http://australianit.news.com.au/articles/0,7204,15450155%5E16123%5E%5Enbv%5E,00.html>> oppure <<http://tinyurl.com/byso4>>

Qui vi è lo stesso identico argomento per quanto concerne il rischio di coltelli appuntiti:

<<http://news.bbc.co.uk/2/hi/health/4581871.stm>>

Il mio commento:

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

** **

Miliardi sprecati in sicurezza antiterrorismo

Di recente sono apparsi svariati articoli che parlano di quanto sia pessima la sicurezza antiterrorismo negli Stati Uniti, di quanti miliardi di dollari sono stati sprecati in sicurezza a partire dall'11 settembre 2001, e di come molto di ciò che è stato acquistato non funziona come promesso.

La prima notizia viene dall'edizione dell'8 maggio del New York Times:

“Dopo aver speso più di 4,5 miliardi di dollari in dispositivi di screening per monitorare i porti, i confini, gli aeroporti, la posta e le linee aeree, il governo federale si sta muovendo per sostituire o modificare gran parte dell'attrezzatura antiterrorismo perché giudicata inefficace, inaffidabile o troppo costosa da gestire.

“Molti degli strumenti di controllo, progettati per rilevare armi da fuoco, esplosivi e armi nucleari e biologiche, sono stati acquistati durante il blitz di spese per la sicurezza immediatamente successivo agli attacchi dell'11 settembre 2001.

“Nel suo tentativo di creare uno scudo virtuale intorno all'America, il Dipartimento per la Sicurezza Nazionale ora prevede di spendere altri miliardi di dollari. Anche se alcuni cambiamenti vengono fatti a causa di tecnologie emerse negli ultimi due anni, molti di essi sono previsti poiché i dispositivi attualmente in uso hanno fatto ben poco per aumentare la sicurezza nazionale, secondo l'esame di documenti di agenzia e di interviste con funzionari federali ed esperti esterni”.

Un altro estratto dell'articolo:

“Fra i problemi: i rilevatori di radiazioni situati nei porti e alle frontiere, che non riescono a distinguere fra le radiazioni emesse da una bomba nucleare e le radiazioni naturali emesse da materiali quotidiani come la lettiera del gatto o da piastrelle di ceramica.

Attrezzature per il monitoraggio aereo nelle principali città solo marginalmente efficaci perché non è stato implementato un numero sufficiente di rilevatori e a volte non sono stati nemmeno installati o calibrati a dovere. Inoltre non producono risultati per intervalli di tempo che possono arrivare a 36 ore -- e nel frattempo un attacco biologico farebbe in tempo ad infettare migliaia di persone.

L'attrezzatura per lo screening agli aeroporti, che i verificatori hanno trovato non essere più efficace di quanto non lo fosse prima che gli ufficiali federali prendessero il controllo della situazione per rilevare se qualcuno sta cercando di introdurre un'arma o un ordigno a bordo di un aereo.

Le macchine del servizio postale, che analizzano solo una piccola percentuale di posta e sono impostate per rilevare antrace ma nessun altro agente biologico.”

Il Washington Post presentava una serie di articoli. Il primo elenca una serie di ulteriori problemi:

"Il contratto per assumere screener di passeggeri agli aeroporti è aumentato da 104 a 741 milioni di dollari in meno di un anno. Gli screener hanno un tasso di fallimento nel rilevare armi più o meno simile a quello immediatamente successivo agli attacchi.

Il contratto per l'acquisto di macchine di rilevazione di esplosivi si è gonfiato a una cifra di almeno 1,2 miliardi di dollari dai 508 milioni iniziali in circa 18 mesi. Le macchine sono state ostacolate dal numero elevato di falsi allarmi.

Un contratto per una rete di computer chiamata US-VISIT per controllare i visitatori stranieri potrebbe costare ai contribuenti 10 miliardi di dollari. Si affida a una tecnologia obsoleta che mette a rischio l'intero progetto.

Le macchine per il rilevamento di radiazioni, costate in totale un mezzo miliardo di dollari e installate per controllare camion e container nei porti e alle frontiere, hanno problemi a distinguere l'uranio arricchito da comuni elettrodomestici. Il problema ha richiesto piani costosi per sostituire questi macchinari."

Il secondo articolo parla della sicurezza alle frontiere e, più recentemente, un articolo del New York Times che parla di come sia scadente la sicurezza nei porti navali.

Vi sono molte ragioni del perché tutto questo sia vero: i problemi del credere a società che hanno qualcosa da venderti, la difficoltà di far funzionare le soluzioni di sicurezza tecnologiche, i problemi legati al fare importanti cambiamenti di sicurezza con rapidità, gli errori di gestione che provengono da ogni burocrazia elefantica come il Dipartimento per la Sicurezza Nazionale, e lo spreco nella difesa di potenziali bersagli terroristici invece di provare ad affrontare ampiamente il terrorismo.

<<http://www.informationclearinghouse.info/article8771.htm>>

<http://www.boston.com/news/nation/washington/articles/2005/05/08/report_says_us_will_discard_upgrade_some_security_devices/>

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

<http://www.washingtonpost.com/wp-dyn/content/article/2005/05/21/AR2005052100778_pf.html>

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

<http://www.washingtonpost.com/wp-dyn/content/article/2005/05/22/AR2005052200613_pf.html>

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

Il New York Times sulla sicurezza nei porti:

<<http://www.navyseals.com/community/articles/article.cfm?id=6954>>

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

Le News di Counterpane

Counterpane offre un nuovo servizio di Identity Management:

<<http://www.counterpane.com/pr-20050613.html>>

Il rapporto dettagliato di Counterpane sull'identity management:

<<http://www.counterpane.com/cgi-bin/whitepaper.cgi>>

Network World sul security monitoring in outsourcing e Counterpane:

<<http://www.networkworld.com/news/2005/061305-outsourcing-security.html>>

Schneier interverrà sul tema della Sicurezza Cibernetica al meeting preparatorio del World Summit for the Information Society (WSIS) il 30 giugno a Ginevra:
<<http://www.itu.int/osg/spu/cybersecurity/>>

** **

Un attacco alla procedura di pairing del protocollo Bluetooth

C'è un nuovo risultato crittografico contro il protocollo Bluetooth. Yaniv Shaked e Avishai Wool dell'Università di Tel Aviv in Israele hanno scoperto come recuperare il PIN controllando la procedura di pairing.

Il pairing è una parte importante del protocollo Bluetooth. È la modalità con cui due dispositivi (un cellulare e l'auricolare, per esempio) si associano l'un l'altro. Generano una chiave segreta condivisa che utilizzeranno per ogni comunicazione futura. È il pairing che fa in modo che i vostri dispositivi Bluetooth, quando siete in una carrozza affollata della metropolitana, non si collegano a tutti gli altri dispositivi presenti.

Secondo le specifiche Bluetooth, i PIN possono essere lunghi fino a 128 bit. Purtroppo molti costruttori si sono standardizzati su un PIN di quattro cifre decimali. Questo attacco può craccare quel PIN di quattro cifre in meno di 0.3 secondi su un vecchio Pentium III a 450 MHz e in 0.06 secondi su un Pentium IV a 3 GHz.

E non è solo una questione di PIN. L'intero protocollo è stato progettato male.

Ad un primo sguardo, questo attacco non è niente di che. Funziona solamente se riuscite a monitorare la procedura di pairing. Il pairing avviene di rado, e in genere nella sicurezza delle mura domestiche o dell'ufficio. Ma gli autori hanno trovato come indurre una coppia di dispositivi Bluetooth a rifare il pairing, permettendo così di intercettare la comunicazione. Loro fingono di essere uno dei due dispositivi, e inviano all'altro un messaggio di chiave di collegamento perduta. Questo induce l'altro dispositivo a gettare la chiave precedente e i due iniziano una nuova sessione di pairing.

Vedendolo nella sua interezza, si tratta di un risultato impressionante. Non sono sicuro, ma presumo che permetterebbe a un aggressore di prendere il controllo dei dispositivi Bluetooth di una persona. Di sicuro permette all'aggressore di mettersi in ascolto sulla rete Bluetooth.

Se uniamo tutto questo allo "sniper rifle" Bluetooth a lungo raggio, si può dire che il protocollo Bluetooth ha un grave problema di sicurezza.

<<http://www.newscientist.com/article.ns?id=dn7461>>

Lo studio:

<<http://www.eng.tau.ac.il/~yash/shaked-wool-mobisys05/index.html>>

Sniper rifle Bluetooth:

<<http://www.tomsnetworking.com/Sections-article106.php>>

** **

Password Safe 2.11

Password Safe è una utility gratuita di archiviazione password per la piattaforma Windows. Di questi tempi, chiunque frequenti il Web con regolarità necessita di ricordare troppe password, ed è impossibile. Ho sempre sostenuto di scriverle tutte su un foglietto e di conservarlo nel portafogli.

Ho realizzato Password Safe come soluzione alternativa. È un piccolo programma che cripta tutte le vostre password usando una passphrase. Il programma è semplice da usare, e non è appesantito da troppe funzionalità inutili. Sicurezza grazie alla semplicità.

Password Safe 2.11 è ora disponibile.

Al momento, Password Safe è un progetto open source a SourceForge, ed è condotto da Rony Shapiro. Ringrazio lui e tutti i programmatori che hanno lavorato al progetto.

La pagina di Password Safe:

<<http://www.schneier.com/passsafe.html>>

La versione 2.11

<https://sourceforge.net/project/showfiles.php?group_id=41019&package_id=33169&release_id=330734> oppure <<http://tinyurl.com/97bm7>>

La pagina del progetto SourceForge:

<<http://passwordsafe.sourceforge.net/>>

Si noti che il mio Password Safe non ha niente a che vedere coi seguenti Password Safe (avrei dovuto scegliere un nome più oscuro per il programma):

<<http://www.passwordsafe.de/eng/>>

<<http://www.fileheaven.com>PasswordSafe/download/8154.htm>>

<<http://www.aptrio.com/Utilities/Desktop-Enhancements/passwordsafe-8929.html>>

È lo stesso di questo, per la piattaforma PocketPC:

<<http://www.pocketpcfreewares.com/en/index.php?soft=1163>>

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

La pubblica divulgazione della perdita dei dati personali

Citigroup ha annunciato la perdita di dati personali di 3,9 milioni di persone. I dati si trovavano in un gruppo di nastri di backup che sono stati inviati tramite UPS (un servizio di corrieri) dal punto A e non hanno mai raggiunto il punto B.

Si tratta di un'enorme perdita di dati, e anche se è improbabile che qualche malintenzionato abbia messo le mani su di essi, questo episodio inciderà profondamente sulla sicurezza di tutti i nostri dati personali.

Potrebbe sembrare che vi sia stata recentemente un'epidemia di perdite di dati sensibili, ma è solo un'apparenza. Quel che stiamo vedendo sono gli effetti di una legge californiana che obbliga le società a divulgare le perdite o i furti di dati sensibili. È sempre successo, solo che ora le società devono dichiararlo al pubblico.

Come esperto di sicurezza, approvo la legge californiana per tre motivi. Primo: i dati sulle effettive intrusioni sono utili per svolgere ricerche. Secondo: avvisare le persone i cui dati sono stati perduti o rubati è una buona idea. Terzo: un più attento esame critico pubblico porta le società a investire più risorse nella protezione dei dati personali.

Pensatelo come un pubblico disonore. Le società investiranno denaro per evitare il costo in Pubbliche Relazioni del pubblico disonore. E quindi la sicurezza migliorerà.

Questo funziona, ma è anche in atto un processo di attenuazione. Più aumentano eventi del genere, meno la stampa ne parlerà. E quando la stampa fa meno rumore, c'è anche un minor pubblico disonore. E quando il pubblico disonore viene meno, diminuisce anche il quantitativo di denaro che le società sono disposte a spendere per evitarlo.

Questa perdita di dati ha già alzato la soglia per i reporter. Furti di dati sensibili ai danni di 50.000 persone non faranno più notizia, e allora non verranno comunicati.

Anche la notifica alle persone che hanno subito la perdita ha un effetto di attenuazione. Conosco gente in California che ha decine di notifiche della perdita dei loro dati personali. Quando la perdita non è seguita da un furto d'identità, le persone iniziano a pensare che non sia un problema vero. E hanno sostanzialmente ragione. Molte perdite di dati sensibili non hanno come conseguenza il furto di identità. Ma questo non vuol dire che non sia un problema.

La divulgazione pubblica è una buona cosa, ma non è sufficiente.

<http://www.businessweek.com/ap/tech/D8AIONPO2.htm?campaign_id=apn_tech_down>
oppure <<http://tinyurl.com/cnj4a>>
<<http://www.informationweek.com/story/showArticle.jhtml?articleID=164301046>> oppure
<<http://tinyurl.com/bcqqp>>
<http://blog.inc.com/archives/2005/06/07/more_lost_data.html>
<http://www.consumeraffairs.com/news04/2005/citigroup_data.html>

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

Prendere in ostaggio i file di un computer

Questo fenomeno è stato previsto da molto tempo. Qualcuno si intrufola nella vostra rete, cripta i vostri file di dati, e poi chiede un riscatto per rilasciare la chiave di decifrazione.

Non so come gli aggressori vi siano riusciti, ma sotto ho delineato quella che forse è la migliore procedura. Si potrebbe programmare un worm per farlo.

1. Introdursi nel computer.
2. Generare una chiave casuale a 256 bit di criptatura file.
3. Criptare la chiave di criptatura file con una comune chiave pubblica RSA.
4. Criptare i file dati con la chiave di criptatura file.
5. Cancellare i file dati e la chiave di criptatura file.
6. Cancellare tutto lo spazio libero su disco.
7. Generare un file contenente la chiave di criptatura file a sua volta criptata-RSA.
8. Chiedere un riscatto.
9. Ricevere il riscatto.
10. Ricevere la chiave di criptatura file criptata.

11. Decifrarla e rispedirla.

Il passo 9 è il più difficile, ed è il punto in cui è più facile esser presi. Non ne so molto di trasferimenti monetari anonimi, ma non credo che i conti svizzeri conservino l'anonimato di un tempo.

Può anche darsi che dobbiate dimostrare di saper decifrare i dati, per cui una semplice modifica è quella di criptare una parte dei dati con un'altra chiave di criptatura file, così da provare alla vittima che siete in possesso della chiave RSA privata.

Gli attacchi in Internet sono cambiati negli ultimi due anni. Non si parla più di hacker, ma di criminali. E dobbiamo aspettarci di vedere questo fenomeno sempre più di frequente in futuro.

<<http://www.cnn.com/2005/TECH/internet/05/24/internet.ransom.ap/index.html>> oppure
<<http://tinyurl.com/cmuox>>

Questo fenomeno è stato previsto da anni:
<<http://www.cryptovirology.com/>>

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

Un'altra minaccia all'antrace si rivela un falso allarme

All'inizio di questo mese, all'ambasciata indonesiana in Australia vi è stata un'altra minaccia all'antrace. Qualcuno ha inviato un po' di polvere bianca in una busta, cosa abbastanza terrificante. Al test successivo è risultata positiva. L'edificio è stato decontaminato e lo staff messo in quarantena per dodici ore. A quel punto i test sono risultati negativi per l'antrace.

Si è riflettuto parecchio su questo falso allarme. Gli aggressori ovviamente sapevano che la loro polvere bianca sarebbe stata velocemente testata per verificare la presenza di un batterio della famiglia del bacillo (della quale l'antrace fa parte), ma che il bacillo avrebbe dovuto essere messo in coltura per due giorni prima che potesse essere effettuata una identificazione più precisa. Perciò, anche senza antrace, sono riusciti a causare due giorni di panico.

A occhio e croce, questo incidente ha avuto qualcosa a che fare con Schapelle Corby (l'ennesima storia legata alla sicurezza). Corby è stata arrestata a Bali con l'accusa di aver introdotto droghe nel paese. In sua difesa (diffusamente creduta in Australia) ha detto di essere stata una vittima inconsapevole dei veri trafficanti di droga. Presumibilmente, i trafficanti lavorano come addetti ai bagagli dell'aeroporto e infilano dei pacchetti di droga in bagagli già controllati per poi recuperarli alla destinazione prima che vengano ridati ai passeggeri. In ogni caso, Bali ha leggi sulla droga molto severe, e Corby è stata recentemente riconosciuta colpevole di ciò che gli australiani chiamano errore giudiziario. Secondo alcuni report della stampa non vi sarebbe alcuna connessione fra i due eventi, ma sembra fin troppo ovvia.

<<http://smh.com.au/articles/2005/06/02/1117568282365.html>>
<<http://news.bbc.co.uk/2/hi/asia-pacific/4598419.stm>>
<<http://www.theage.com.au/text/articles/2005/06/04/1117825103781.html>>
oppure <<http://tinyurl.com/9pujh>>

350 falsi allarmi:
<<http://www.smh.com.au/news/National/PM-embassy-attack-makes-it-harder-for-Corby/2005/06/01/1117568262312.html>> oppure <<http://tinyurl.com/atd6a>>

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

Commenti dei lettori

Da: "Dave Mortensen" <drmort@flash.net>

Oggetto: Il suo articolo del 10 maggio

Ho trovato molto interessante il suo appello per porre un freno agli abusi di sorveglianza elettronica, ma vorrei far notare un fraintendimento piuttosto comune a riguardo della sorveglianza e dell'uso di prove.

Se da un lato è apparentemente illegale spiare qualcuno senza un mandato, sta di fatto che gli agenti delle forze dell'ordine e gli investigatori privati ricorreranno a questo se lo ritengono necessario -- ben sapendo di non poter rivelare come hanno ottenuto l'informazione e di non poter presentare alcuna prova ottenuta con tale metodo in un processo o in una causa civile.

Scoprire qualcosa grazie a queste intrusioni e non poter utilizzare le informazioni ottenute "illegalmente" non è necessariamente un serio ostacolo per una indagine. Vi può essere un valore strategico significativo nel semplice ottenimento di informazioni relative all'esistenza di altre prove potenziali o di testimoni che possano produrre prove ancora migliori, per le quali mostrare un percorso appropriato di acquisizione e custodia.

Come analogia, consideri che cosa succede quando un legale o una società di recupero crediti sono determinati a scoprire i beni "nascosti" di una persona che si trova con una sentenza pendente o che ha presentato istanza di protezione per bancarotta. Il legale o la società presumono che ci sia sotto una frode, e assumono un investigatore. Quell'investigatore non deve ottenere un mandato -- infatti tutto quel che deve fare è trovare il denaro o i beni. Il telefono o il computer vengono messi (illegalmente) sotto controllo e alla fine l'investigatore scopre che il tesoro nascosto esiste davvero. Questo è sufficiente. Una soffiata "anonima" passa le informazioni al legale o alla società di recupero crediti e con queste l'imputato si trova con le spalle al muro e l'accusa federale di falsa testimonianza. Le strade sono due: o ammette tutto e paga, o nega e l'informazione passa all'ufficio del Procuratore (o all'IRS).

Più diffuse sono le reti illegali di informatori, un po' come Orazio Lembo Jr., che ha tenuto in pugno per quattro anni impiegati di banca (manager) e un manager di un'agenzia di collocamento del New Jersey, offrendo qualsiasi tipo di informazione richiesta dai suoi "clienti" e pagando gli infiltrati 10 dollari a colpo. Fra i clienti di Lembo c'erano procuratori e società di recupero crediti. Ha guadagnato milioni giocando al detective. La sua rete di contatti ha davanti anni di prigione. Chissà gli studi legali e le società di recupero crediti che lo hanno fatto ricco a che cosa si attaccheranno per accusarlo... forse a nulla.

E dato che la prevenzione, e non solo la prosecuzione, è una delle ragioni nelle problematiche antiterrorismo, il ruolo di ago della bilancia giocato dalle autorità nel decidere quando e se ottenere un mandato lascia un gran numero di vittime di violazione della privacy che potrebbero non essere mai accusate di nulla. Dato che le informazioni raccolte saranno inserite alla fine in qualche sistema di analisi e raccolta dati dei cittadini (e potenzialmente saranno consultate senza autorizzazione o rubate, come nel caso Seisint), non c'è davvero alcuna prospettiva di protezione della privacy allo stato attuale delle cose.

I "meccanismi corrispondenti per frenare gli abusi" che lei richiede dovrebbero comprendere gravi sanzioni penali non solo ai danni delle forze dell'ordine, che violano la legge che esige un mandato di perquisizione, ma anche ai danni dei vari "detective" e delle società che richiedono continuamente di ottenere informazioni sulle persone.

Da: Paul Schumacher <psch@optonline.net>

Oggetto: Re: Rilevare materiale nucleare in transito

Ho l'hobby di raccogliere, studiare e fotografare minerali di uranio e thorio (<http://www.uraniumminerals.com>). Una delle cose che faccio è quella di misurare la radioattività di ogni campione. Utilizzo un contatore Geiger digitale tenuto a una distanza di 2,5 cm dal campione.

Ho alcuni campioni molto caldi, uno raggiunge i 150 microseivert all'ora. Altri sono appena superiori a un segnale di fondo. Ci vuole mezz'ora di assestamento per ottenere una buona lettura da questi ultimi. L'uranio purificato è meno radioattivo, grammo per grammo, dell'uranio di questi campioni dato che non presenta molti dei sottoprodotti (il radio) del decadimento dell'uranio.

La schermatura può essere d'aiuto, ma l'efficacia della schermatura dipende dalla massa. Un'arma nucleare dovrà essere rivestita da almeno dieci centimetri di piombo per essere protetta da rilevamenti casuali. E questo significa dover spedire un pacco molto pesante.

Invece di schermare la bomba da possibili rilevamenti, è molto più probabile che l'avversario cercherà di introdurla o alla maniera degli immigranti messicani, o via sottomarino, come gli agenti tedeschi durante la Seconda Guerra Mondiale. Più sensori mettiamo, più diventano appetibili metodi alternativi.

Da questo possiamo trarre delle conclusioni:

1. Un ordigno nucleare di nuova fabbricazione e di ottima progettazione produrrà ben poche radiazioni.
2. La schermatura può rendere difficile rilevare l'ordigno, ma la massa stessa della schermatura tradirà la presenza dell'arma.
3. I rilevatori situati in postazioni fisse verranno semplicemente aggirati.
4. Se non possiamo salvaguardare le nostre frontiere dai trafficanti di droga e dagli immigranti, come possiamo proteggerci contro Armi di Distruzione di Massa?
5. Se anche riuscissimo a rilevare il 100% di tutto il materiale nucleare, a prescindere da come è schermato, ciò non servirebbe a fermare un attacco che fa uso di agenti chimici o biologici.

Ora a tutto questo aggiungiamoci le tonnellate di cibo, merci e posta che arrivano anche solo in una cittadina di 25.000 abitanti e le merci, la posta, e la spazzatura che ogni giorno esce dalla città.

Ora pensiamo alle nostre città più grandi. Per avere un maggior numero di vittime e per creare un danno economico maggiore, un attacco terroristico nucleare non è necessario che avvenga nel cuore della città. Se viene rilevato e bloccato, che cosa potrebbe fermare un controllo e una detonazione remoti prima di poter disinnescare l'ordigno?

È come fermare un'autobomba. La risposta per prevenire un eventualità del genere manca, un'arma nucleare pone semplicemente i risultati a un livello più alto di distruzione.

Anche se utili, i rilevatori di radiazioni non riusciranno a fermare un attacco terroristico nucleare. A fermarlo deve essere un piccolo componente di un sistema di sicurezza meglio integrato.

Da: Rich Wilson <wk633@yahoo.com>

Oggetto: Re: REAL ID

Sarà interessante vedere come questo si rivolgerà a vari gruppi "marginali":

1) Le persone che non hanno la patente di guida. Mia moglie non ne ha una. Io non mi sono preoccupato di averne una prima dei 26 anni. Il fatto che mia moglie non l'abbia si è dimostrato interessante quando un agente di polizia ha minacciato di farle una multa per aver attraversato la strada fuori dalle strisce pedonali. Di fronte all'indifferenza di mia moglie, egli le ha fatto notare che la cosa avrebbe influito sulla sua patente. A quel punto lei se ne è beatamente fregata!

2) Le persone che hanno come indirizzo un numero di casella postale. Santa Barbara ha una comunità di "campeggiatori" piuttosto grande, che vaga da parcheggio a parcheggio, malgrado gli sforzi della città per indurli ad andarsene.

3) Le persone con patenti revocate. Forse si troverà il rimedio a questo modificando il loro status nel magico database?

4) Le persone con residenze in più di uno stato. REAL ID non permette licenze multiple, e al momento alcuni stati obbligano ad avere una licenza per il loro stato.

Da: Petri Aukia <petri@aukia.com>
Oggetto: Re: REAL ID

Vi è una sottile differenza, da lei non menzionata, fra le patenti di guida americane ed europee e le loro conseguenze sulla privacy.

Le patenti finlandesi e francesi (e molto probabilmente tutte le altre della Comunità Europea) non riportano l'indirizzo di casa del conducente. Servono a documentare la tua esistenza, il tuo nome, la tua foto, la tua firma, il numero di previdenza sociale, e il tipo di veicoli che sei abilitato a guidare. Pittogrammi, numeri e disposizioni dei dati sono standardizzati, per cui un agente di pattuglia può leggere la patente di guida di qualsiasi nazione della UE.

Ogni paese ha un meccanismo per far derivare l'indirizzo del conducente dal numero di previdenza sociale o da un dato equivalente, ma questo è a disposizione solo del governo e delle aziende a cui tu hai dato la possibilità di conoscere il tuo indirizzo (giornali, riviste, e simili).

Da: Julien.Maisonneuve@alcatel.com
Oggetto: L'Europa e il furto d'identità

In aggiunta a quanto da lei accennato in merito alle strutture legali europee atte a proteggere i dati sensibili (che non sono affatto complete e predominanti attraverso la comunità come uno vorrebbe), la stessa nozione di "furto d'identità" è pressoché sconosciuta in Europa. Vi sono molte cause, molte legate ai benefici assai limitati che uno può ottenere dall' "identità" in sé. Ciò include l'assenza di posizione creditizia esistente negli USA, e procedure diverse per l'apertura di conti bancari e di ottenimento dell'accesso alle loro risorse.

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

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

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

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

La versione italiana è curata da Communication Valley SpA <http://www.communicationvalley.it/>.
Per iscriversi o cancellarsi andare all'indirizzo <http://www.cryptogram.it/>.
I numeri arretrati sono disponibili all'indirizzo <http://www.cryptogram.it/>.
Per informazioni crypto-gram@communicationvalley.it.

Inoltrate liberamente CRYPTO-GRAM a colleghi ed amici che possano trovare questa pubblicazione di un certo interesse. Viene concessa l'autorizzazione a ristampare CRYPTO-GRAM, a condizione che sia stampata integralmente.

CRYPTO-GRAM è realizzata da Bruce Schneier. Schneier è l'autore dei best seller "Beyond Fear", "Secrets and Lies" [tradotto in Italia col titolo "Sicurezza Digitale"] e "Applied Cryptography", e inventore degli algoritmi Blowfish, Twofish e Yarrow. È il fondatore e CTO di Counterpane Internet Security, Inc., e membro del comitato consultivo dell'Electronic Privacy Information Center (EPIC). Scrive spesso e tiene conferenze in merito alla sicurezza informatica e alla crittografia. Il suo sito Web è all'indirizzo <<http://www.schneier.com>>.

Counterpane Internet Security, Inc. è leader mondiale nel monitoraggio guidato della sicurezza informatica. Gli analisti esperti in sicurezza di Counterpane proteggono reti per aziende inserite nella Fortune 1000 a livello mondiale.

Copyright (c) 2005 by Bruce Schneier.