

CRYPTO-GRAM
15 ottobre 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>
<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.

Per consultare i numeri arretrati, o per iscriversi, andare all'indirizzo: <http://www.schneier.com/crypto-gram.html>.

Oppure si può leggere il presente numero direttamente sul Web, all'indirizzo:
<http://www.schneier.com/crypto-gram-0610.html>.

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

Crypto-Gram è anche consultabile in formato RSS.

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

In questo numero:

Effettuare lo screening di persone con autorizzazioni speciali
Hezbollah ha intercettato le comunicazioni crittografate della
radio militare israeliana?

Rinnovate adesso il vostro passaporto!

Informazioni erronee e il caso Arar

Le ristampe di Crypto-Gram

Macchine fotografiche costose nel bagaglio fatturato

Facebook e il controllo dei dati

Tolto il segreto sugli indici delle pubblicazioni NSA, ora sono
online

News

Il pupillometro

Piccoli display sulle smart card

Cellulari che strillano

Le news di Counterpane

Novità su FairUse4WM

Software per il voto elettronico e segretezza

La legge sulla tortura in forma di codice C

Il Canile: SecureRF

Hacking ai danni del Bureau of Industry and Security

Le reti universitarie e la sicurezza dei dati

Commenti dei lettori

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

Effettuare lo screening di persone con autorizzazioni speciali

Perché si dovrebbe perder tempo ai checkpoint di sicurezza aeroportuali per effettuare lo screening di persone in possesso di autorizzazioni speciali rilasciate dal governo degli Stati Uniti? Questa domanda, perfettamente sensata, è stata posta di recente da Robert Poole, direttore del dipartimento di ingegneria dei trasporti alla Reason Foundation, mentre lui e il sottoscritto venivano intervistati dalla WOSU Radio in Ohio.

Secondo Poole, le persone munite di autorizzazioni speciali governative, persone a cui vengono affidati segreti di sicurezza nazionale statunitense, hanno sufficiente affidabilità per poter passare la sicurezza negli aeroporti con uno screening veloce e sommario. Sono state già sottoposte a vari background check, ha dichiarato Poole, e sarebbe più efficiente concentrare risorse di screening sul resto dei passeggeri.

Per chi non è un addetto ai lavori in ambito di sicurezza, questo è un ragionamento assolutamente sensato. Ma si tratta di una pessima idea, e il comprenderne i motivi ci insegna alcune lezioni importanti sulla sicurezza.

La prima lezione è che la sicurezza è un sistema. Identificare la speciale autorizzazione di un individuo è un procedimento complicato. Le persone con autorizzazioni speciali non possiedono documenti di identità particolari, e non possono semplicemente avere accesso a infrastrutture protette. Un'autorizzazione viene mantenuta da una determinata organizzazione (solitamente quella per cui tali persone lavorano) e viene trasferita ad altre organizzazioni, mediante una comunicazione segreta, quando l'impiegato viaggia per lavoro in veste ufficiale.

I checkpoint di sicurezza negli aeroporti non sono attrezzati per ricevere queste comunicazioni segrete, perciò occorrerebbe sviluppare un altro sistema.

Ovviamente, per la persona con autorizzazione speciale, non ha senso che il proprio ufficio invii un messaggio a ogni aeroporto dell'itinerario durante il viaggio. Più semplice sarebbe avere un database centralizzato di persone munite di autorizzazioni particolari. Ma si dovrebbe realizzare questo database. E proteggerlo. E assicurarsi che venga mantenuto aggiornato.

O forse si potrebbe creare un nuovo tipo di documento d'identità, un documento che identifichi le persone con speciali autorizzazioni. Ma anche in questo caso sarebbe necessario un database backend e una tessera che non possa essere falsificata. E le autorizzazioni possono essere revocate in qualsiasi momento, per cui occorre che esista un qualche sistema per invalidare i documenti automaticamente e da remoto.

In qualunque modo si intenda procedere, è necessario implementare un nuovo insieme di procedure di sicurezza ai checkpoint degli aeroporti per gestire queste persone. Le procedure devono essere sufficientemente valide in modo da evitare possibili inganni. Gli screener devono essere addestrati. Il sistema deve essere collaudato.

Quel che sembrava un'idea semplice (non sprecare tempo a controllare persone munite di speciali autorizzazioni governative) si trasforma in breve tempo in un complicato sistema di sicurezza con ogni genere di nuove vulnerabilità.

La seconda lezione è che la sicurezza è un compromesso. Non abbiamo a disposizione una quantità infinita di denaro da investire sulla sicurezza. Occorre decidere in cosa investire tale denaro, e la scelta

migliore sono le soluzioni che garantiscono maggiore sicurezza in rapporto al denaro speso.

Considerato il fatto che pochissimi cittadini americani possiedono speciali autorizzazioni, e che controllarli più velocemente ai checkpoint non rappresenta poi questo grande vantaggio per chi attende in coda, non sarebbe più intelligente investire il denaro altrove? Anche se si stessero considerando compromessi di sicurezza limitati ai soli checkpoint aeroportuali, io preferirei prendere le centinaia di milioni di dollari che verrebbe a costare questo sistema e li investirei in nuovi screener di sicurezza e nell'addestramento di quelli che già stanno lavorando. Così facendo si accorcerebbero le code e gli screener sarebbero maggiormente efficienti, un doppio vantaggio.

La terza lezione è che spesso le decisioni di sicurezza si basano su priorità del tutto soggettive. Suppongo che Poole sia in possesso di un'autorizzazione speciale (è stato un membro del team di transizione Bush-Cheney nel 2000) e che per lui sia una seccatura sottoporsi alle stesse procedure di screening riservate a tutti gli altri comuni passeggeri con i quali è costretto a stare in coda all'aeroporto. Dal suo punto di vista non controllare individui come lui è una cosa ovvia. Oggettivamente non lo è affatto.

Questo discorso è analogo al controllare i piloti d'aereo, una cosa che suscita regolarmente grande ilarità fra i non esperti di sicurezza. Quel che non comprendono è che il problema non è se fidarsi o meno dei piloti, dei tecnici di manutenzione o delle persone con speciali autorizzazioni. La questione è fidarsi o meno di persone vestite da piloti, o in possesso di tesserini da tecnico di manutenzione, o che dichiarano di avere speciali autorizzazioni.

Le scelte sono due: o si costruisce un'infrastruttura che verifichi tali asserzioni, oppure si presume che siano false. E, con le dovute scuse ai piloti, ai tecnici e alle persone con autorizzazioni speciali, è più semplice, economico e sicuro controllarli tutti quanti.

Questo articolo è originariamente apparso su Wired.com.
<http://www.wired.com/news/columns/1,71906-0.html>

** *** *****

Hezbollah ha intercettato le comunicazioni crittografate della radio militare israeliana?

Secondo Newsday:

"I guerriglieri di Hezbollah sono riusciti a intercettare le comunicazioni radio israeliane durante le battaglie avvenute in Libano il mese scorso, una svolta decisiva a livello di intelligence che, secondo ufficiali di Hezbollah e libanesi, ha contribuito a vanificare gli assalti dei carri armati israeliani.

"Utilizzando una tecnologia fornita molto probabilmente dall'Iran, dei team speciali di Hezbollah hanno monitorato le frequenze radio in costante variazione delle truppe israeliane di terra. Ciò ha permesso ai guerriglieri di avere un'idea abbastanza chiara dei movimenti, dei rapporti sui caduti e delle rotte degli approvvigionamenti israeliani. Secondo gli ufficiali, ha inoltre permesso alle unità anticarro di Hezbollah di prendere di mira più efficacemente i mezzi corazzati israeliani in avanzamento.

Si legga l'articolo. In sostanza, il problema è un errore operativo:

"Con il frequency hopping e la crittografia, gran parte delle comunicazioni radio risultano assai difficili da decodificare, ma a volte le truppe sul campo di battaglia commettono degli errori nel seguire le procedure radio protette, e possono fornire al nemico il modo di penetrare negli schemi di frequency hopping. È quanto può essere accaduto durante alcune battaglie fra Israele e Hezbollah, secondo il funzionario Libanese. È inoltre probabile che le squadre di Hezbollah avessero sofisticati dispositivi di ricognizione in grado di intercettare segnali radio anche durante il frequency hopping".

Sono d'accordo con The Register: "Le dichiarazioni secondo cui i combattenti di Hezbollah hanno potuto sfruttare tale intelligence per ottenere informazioni sui movimenti delle truppe e sulle rotte degli approvvigionamenti sono plausibili, almeno per i profani, tuttavia dovrebbero essere trattate con una certa cautela, visto che sono di fatto confermate solo da fonti anonime".

Personalmente nutro uno scetticismo ancora maggiore. Se davvero Hezbollah è stato in grado di fare tutto questo, l'ultima cosa che Hezbollah vorrebbe è che la stampa ne parli. Ma se Hezbollah non può farlo, allora ben vengano le storie di disinformazione.

<<http://www.newsday.com/news/printedition/stories/ny-wocodel184896831sep18,0,7091966,print.story>> oppure <<http://tinyurl.com/jncdk>>
<http://www.theregister.co.uk/2006/09/20/hezbollah_cracks_israeli_radio/>

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

Rinnovate adesso il vostro passaporto!

Se possedete un passaporto, ora è il momento di rinnovarlo, anche se non sta per scadere nell'immediato. Se non avete un passaporto e pensate di richiederlo, fatelo adesso. In molti paesi, Stati Uniti compresi, nei passaporti verrà presto incorporato un chip RFID. Ed è molto meglio non avere uno di quei chip nel passaporto.

RFID sta per Radio Frequency IDentification (identificazione mediante radiofrequenze). I passaporti dotati di chip RFID conservano in memoria una copia elettronica delle informazioni del passaporto: il vostro nome, una fototessera digitale, eccetera. E in futuro il chip potrebbe memorizzare le vostre impronte digitali o visti digitali di vari paesi.

Di per sé, questo non è un problema. Ma i chip RFID non devono essere inseriti in un lettore per funzionare. Analogamente ai chip utilizzati sui Telepass autostradali, essi operano per prossimità. Il rischio è dunque rappresentato dalla possibilità di accesso clandestino: le vostre informazioni sul passaporto potrebbero essere lette a vostra insaputa e senza il vostro permesso da un governo che sta cercando di tracciare i vostri movimenti, da un criminale intenzionato a rubarvi l'identità o da qualcuno semplicemente curioso di conoscere la vostra cittadinanza.

Inizialmente il Dipartimento di Stato ha minimizzato tali rischi, ma in risposta a varie critiche da parte di esperti ha implementato alcune funzionalità di sicurezza. I passaporti avranno una custodia protettiva che renderà più difficile la lettura delle informazioni quando il passaporto è chiuso. E ora sono stati aggiunti meccanismi di controllo di accesso e di crittografia che dovrebbero rendere più difficoltosa la raccolta, la comprensione e l'alterazione dei dati da parte di un

lettore non autorizzato.

Pur contribuendo alla protezione dei dati, queste contromisure non sono sufficientemente profonde. La custodia protettiva serve a poco quando il passaporto viene aperto. Basta viaggiare all'estero per rendersi conto di quanto spesso sia necessario mostrare il passaporto: negli alberghi, nelle banche, negli Internet café. Chiunque sia intenzionato a raccogliere i dati dei passaporti potrebbe implementare un lettore in uno qualsiasi di quei luoghi. E malgrado il Dipartimento di Stato insista nel sostenere che il chip può essere letto solo da un lettore distante pochi centimetri, i chip sono stati letti anche da molti metri di distanza.

Anche gli altri meccanismi di sicurezza sono vulnerabili, e molti ricercatori di sicurezza hanno già trovato delle falle. Uno ha scoperto che poteva individuare singoli chip mediante certe caratteristiche peculiari delle trasmissioni radio. Un altro è riuscito a clonare un chip senza problemi. Il Dipartimento di Stato ha definito tutto questo una "bravata senza senso", facendo presente che il ricercatore non era in grado di leggere o modificare i dati. Ma il ricercatore in questione ha raggiunto il suo risultato solo dopo due settimane di tentativi; la sicurezza del vostro passaporto deve essere sufficientemente robusta da durare almeno dieci anni.

Questo è forse il rischio maggiore. I meccanismi di sicurezza sul vostro passaporto devono durare per lo meno quanto il passaporto stesso. Credere che la sicurezza del passaporto rimarrà sicura per un tale intervallo di tempo è ridicolo quanto pensare che non vi sarà nel frattempo un altro aggiornamento di sicurezza per Microsoft Windows. I miglioramenti della tecnologia delle antenne aumenteranno sicuramente la distanza dalla quale è possibile leggere un passaporto e potranno addirittura permettere a lettori non autorizzati di penetrare la custodia protettiva.

Qualunque cosa accada, se avete un passaporto con un chip RFID, siete nei guai. Anche se basta mettere il passaporto nel forno a microonde per disabilitare il chip, il rivestimento protettivo farà letteralmente scintille. E malgrado gli Stati Uniti hanno dichiarato che un chip non funzionante non invaliderà un passaporto, non è chiaro se ciò varrà anche nel caso di un chip danneggiato volontariamente.

L'ufficio passaporti dello stato del Colorado sta già rilasciando passaporti RFID e il Dipartimento di Stato si aspetta che gli uffici passaporti di tutti gli Stati Uniti facciano altrettanto entro la fine dell'anno. Molti altri paesi sono in procinto di passare a questo sistema, quindi rinnovate/richiedete il passaporto prima che sia troppo tardi. Con un passaporto rinnovato ancora di tipo tradizionale, potete aspettare 10 anni prima di avere un passaporto RFID, quando la tecnologia sarà più matura, quando avremo una migliore comprensione dei rischi di sicurezza e quando vi saranno altre tecnologie da poter sfruttare per limitare i rischi. Meglio non fare da cavie adesso.

Questo articolo di opinione è apparso originariamente nel Washington Post.

<http://www.washingtonpost.com/wp-dyn/content/article/2006/09/15/AR2006091500923.html>

Confutazione:

<http://www.mercurynews.com/mld/mercurynews/news/opinion/15637460.htm>

I miei precedenti scritti in merito ai passaporti RFID:

http://www.schneier.com/blog/archives/2006/08/hackers_clone_r.html

http://www.schneier.com/blog/archives/2004/10/rfid_passports.html
http://www.schneier.com/blog/archives/2005/04/rfid_passport_s.html
<http://www.schneier.com/essay-060.html>
http://www.schneier.com/blog/archives/2005/08/rfid_passport_s_1.html

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

Informazioni erronee e il caso Arar

Maher Arar è un cittadino canadese originario della Siria. Il 26 settembre 2002 ha cercato di volare dalla Svizzera a Toronto. Di scalo a New York per cambiare volo, è stato trattenuto dalle autorità Statunitensi, quindi rispedito in Siria, dove è stato torturato. Questa persona è innocente al 100%.

Il governo canadese ha ultimato la sua "Commissione di Inchiesta sull'Operato dei Funzionari Canadesi in Relazione a Maher Arar" ("Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar"), i cui risultati sono di pubblico dominio. Dal comunicato stampa: "Su Maher Arar, il Sovrintendente è giunto a un'importante conclusione: 'Posso affermare categoricamente che non vi sono elementi che provino che il Sig. Arar abbia commesso alcun reato o che le sue attività costituiscano una minaccia per la sicurezza del Canada'".

Sicuramente è una cosa su cui dovrebbero riflettere tutti coloro che sostengono il diritto da parte degli USA di trattenere e torturare degli individui senza dover dimostrarne le colpe. Ma quel che può essere più interessante per i lettori di questa newsletter è il ruolo giocato dalle informazioni erronee nella deportazione e successiva tortura di un uomo innocente.

Privacy International riassume il rapporto. I seguenti sono alcuni dei loro punti essenziali:

"La RCMP ha fornito agli Stati Uniti un intero database di informazioni relative a un'indagine antiterrorismo (3 CD di informazioni), in una modalità non conforme alle linee di condotta della RCMP che richiedono verifiche di pertinenza, affidabilità, e presenza di informazioni personali. Questa azione è stata, di fatto, senza precedenti.

"La RCMP ha fornito agli Stati Uniti informazioni erronee sul conto di Arar, tali da metterlo ingiustamente in cattiva luce e tali da esagerare la sua importanza nei confronti di un'indagine della RCMP. Sono state allegate alcune 'note erronee'.

"Mentre Arar veniva trattenuto negli Stati Uniti, la RCMP ha fornito informazioni a suo riguardo al Federal Bureau of Investigation (FBI), 'alcune delle quali restituivano un ritratto sbagliato e ingiusto della persona'. La RCMP ha fornito alle autorità statunitensi informazioni imprecise, che tendevano a collegare Arar ad altri sospetti terroristi; e ha riferito alle autorità statunitensi che Arar aveva precedentemente rifiutato di essere interrogato (altra informazione inesatta); e la RCMP ha altresì dichiarato che poco dopo il rifiuto di tale interrogatorio, Arar aveva improvvisamente lasciato il Canada per recarsi in Tunisia, 'La dichiarazione riguardante il rifiuto a essere interrogato ha avuto il potere di destare il sospetto, specie presso ufficiali delle forze dell'ordine, che il Sig. Arar avesse qualcosa da nascondere'. I dati forniti alle autorità statunitensi da parte della RCMP inoltre collocavano Arar nelle vicinanze di Washington DC l'11 settembre 2001, mentre in realtà egli si trovava in California".

La supervisione giudiziaria è un meccanismo di sicurezza. Va a impedire che la polizia imprigioni la persona sbagliata. Il punto dell'habeas corpus è che la polizia deve presentare le prove di fronte a una terza parte neutrale, e non trattenere indefinitamente o torturare qualcuno solo perché lo ritiene colpevole. Tutti siamo meno al sicuro se mitigiamo queste misure di sicurezza.

Il background:

<[http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-543297](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-543297)
> oppure <<http://tinyurl.com/yl4s9y>>

Il rapporto governativo:

<<http://www.ararcommission.ca/eng/index.htm>>
<http://www.ararcommission.ca/eng/ReleaseFinal_Sept18.pdf>

Privacy International:

<[http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-543296](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-543296)
> oppure <<http://tinyurl.com/yfd6zb>>

La supervisione giudiziaria:

<<http://www.schneier.com/essay-045.html>>

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

Le ristampe di Crypto-Gram

Crypto-Gram è attualmente al suo nono anno di pubblicazione. I numeri precedenti coprono tutta una serie di argomenti legati alla sicurezza e si possono trovare 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).

Il phishing:

<<http://www.schneier.com/crypto-gram-0510.html#1>>

Il rapporto del Gruppo di Lavoro di Secure Flight

<<http://www.schneier.com/crypto-gram-0510.html#10>>

Il giudice Roberts, la privacy e il futuro

<<http://www.schneier.com/crypto-gram-0510.html#16>>

Mantenere segrete le interruzioni di un servizio:

<<http://www.schneier.com/crypto-gram-0410.html#2>>

I passaporti RFID:

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

L'eredità del DES:

<<http://www.schneier.com/crypto-gram-0410.html#8>>

La sorveglianza all'ingrosso:

<<http://www.schneier.com/crypto-gram-0410.html#10>>

<<http://www.schneier.com/crypto-gram-0410.html#11>>

La libertà accademica e la sicurezza:

<<http://www.schneier.com/crypto-gram-0410.html#13>>

Il futuro della sorveglianza:

<http://www.schneier.com/crypto-gram-0310.html#1>

La strategia nazionale per rendere sicuro il Cyberspazio:

<http://www.schneier.com/crypto-gram-0210.html#1>

Cyber-terrorismo:

<http://www.schneier.com/crypto-gram-0110.html#1>

I pericoli della porta 80:

<http://www.schneier.com/crypto-gram-0110.html#9>

Attacchi semantici:

<http://www.schneier.com/crypto-gram-0010.html#1>

La NSA sulla sicurezza:

<http://www.schneier.com/crypto-gram-0010.html#7>

"Così vorresti diventare un crittografo":

<http://www.schneier.com/crypto-gram-9910.html#SoYouWanttobeCryptographer> oppure <http://tinyurl.com/8tk8t>

Lunghezza delle chiavi e sicurezza:

<http://www.schneier.com/crypto-gram-9910.html#KeyLengthandSecurity>

Steganografia: verità e fantasie:

<http://www.schneier.com/crypto-gram-9810.html#steganography>

Appunti per gli apprendisti scrittori di cifrati:

<http://www.schneier.com/crypto-gram-9810.html#cipherdesign>

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

Macchine fotografiche costose nel bagaglio fatturato

Questa entrata di un blog tratta i problemi che insorgono quando si è costretti a lasciare macchine fotografiche costose nel bagaglio fatturato su un aereo:

"Beh, avendo vissuto più di 12 anni a Kashmir, sono decisamente abituato a questo tipo di sicurezza. È dal 1990 che qui non è possibile portare bagaglio a mano. Non è nemmeno possibile lasciare batterie in nessun dispositivo, che venga fatturato o meno. Almeno ci è stata data la possibilità di portare a bordo computer portatili, e recentemente anche di utilizzarli (con le batterie). Ma se le cose continuano a muoversi in questa direzione, e non ho dubbi a riguardo, dobbiamo iniziare a pensare a come fatturare le nostre fotocamere e computer, e a come farlo in maniera sicura. È un'idea molto sgradevole. Due anni fa ordinai una Canon 20D e chiesi a un'amica di incontrarci in Inghilterra e di portarmela "a mano". La mia amica la sistemò nel suo bagaglio fatturato. Quella borsa non fu più ritrovata. L'amica non era assicurata e tutto ciò che ottenni furono 100 dollari dalla British Airways per la fotocamera e 500 dollari dall'American Express (buyer protection), nient'altro. E adesso sembra quasi che dobbiamo iniziare a fatturare le nostre fotocamere e i nostri computer involontariamente. Bene, ecco alcune idee."

Tutte cose basilari, e tutti noi siamo a conoscenza dei rischi che corriamo quando mettiamo oggetti costosi e di valore nel bagaglio fatturato.

La parte interessante è uno dei commenti al blog, a circa metà della

pagina. Un altro fotografo si domanda se le normative TSA in merito alle armi da fuoco possano essere estese alle attrezzature fotografiche:

"Perché non fare semplicemente in modo che la TSA adotti le stesse regolamentazioni sul check-in di armi da fuoco anche per le attrezzature foto/video?"

"Tutte le armi da fuoco devono essere disposte nel bagaglio fatturato, niente bagaglio a mano."

"Tutte le armi da fuoco devono essere trasportate in una valigetta rigida con chiusura a chiave autorizzata non-TSA. Ciò per impedire l'apertura della valigia successivamente ai controlli di sicurezza."

"Dopo aver portato l'attrezzatura allo sportello della linea aerea e averne dichiarato e mostrato i contenuti al rappresentante della linea aerea, la valigia deve essere portata al checkpoint della TSA dove viene controllata da uno screener, richiusa davanti a voi, vi vengono riconsegnate le chiavi (se non si tratta di una chiusura a combinazione), e il bagaglio disposto direttamente sul rullo trasportatore per essere caricato sull'aereo."

"All'esterno della valigia (o della borsa, se l'attrezzatura viene collocata all'interno di qualcos'altro) non vengono applicati marchi, adesivi o etichette che possano identificare il contenuto."

"Potrebbe essere la soluzione al problema? Non ho mai perso un'arma viaggiando in aereo".

Poi qualcun altro propone un suggerimento brillante: mettere un arma da fuoco insieme all'attrezzatura fotografica:

"Si definisce 'arma' un fucile, una doppietta, una rivoltella, una pistola ad aria e una PISTOLA STARTER. Sì, proprio quelle piccole pistole che sparano un colpo a salve per dare il via a una gara su pista o di nuoto, vengono considerate armi... e NON necessitano di registrazione in nessuno stato degli USA."

"Ho una pistola starter per ognuna delle mie valigette. Tutto quel che devo fare al check-in è dire all'impiegato che ho un'arma da dichiarare... Mi viene data una schedina da firmare, la schedina viene messa nella valigetta, la valigetta viene consegnata a un funzionario della TSA che prende la mia chiave, chiude la valigetta, e mi restituisce la chiave."

"Questa è la procedura. La valigetta viene super-controllata e tenuta d'occhio... La TSA non vuole che si perda una valigetta contenente un'arma. Pertanto, le possibilità che il bagaglio vada perduto sono virtualmente zero."

"È un ottimo sistema quando si viaggia con la propria attrezzatura fotografica... Sto facendo così dal dicembre 2001 e non ho mai avuto alcun problema".

Devo ammettere di essere impressionato da questa soluzione.

http://blogs.lexar.com/mattbrandon/2006/08/tighter_security.html

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

Facebook e il controllo dei dati

All'inizio di questo mese Facebook, il noto sito di social networking, ha imparato una dura lezione in merito alla privacy. Ha introdotto una nuova funzione chiamata "News Feeds" che visualizza un'aggregazione di tutte le azioni che i membri intraprendono sul sito: aggiungere e cancellare amici, modificare lo stato di un rapporto, indicare una nuova canzone preferita, un nuovo interesse, ecc. Gli amici di un utente non devono più visitare la sua pagina per vedere i cambiamenti: tali modifiche vengono loro presentate in automatico.

L'indignazione è stata grandissima. Un gruppo, Students Against Facebook News Feeds, ha raccolto più di 700.000 membri per andare a protestare direttamente alla sede centrale della compagnia. Il fondatore di Facebook era totalmente sbalordito, e la compagnia si è affrettata ad aggiungere alcune opzioni di privacy.

Benvenuti nel mondo confuso e complicato della privacy nell'era dell'informazione. Facebook non pensava che vi sarebbero stati dei problemi: tutto quel che ha fatto è stato prendere dei dati già a disposizione e aggregarli in un nuovo formato per realizzare ciò che ha percepito poter essere un vantaggio per i propri clienti. I membri di Facebook hanno capito istintivamente che rendere tali informazioni più semplici da visualizzare faceva un'enorme differenza, e che la privacy riguarda maggiormente il controllo e non la segretezza.

D'altra parte, gli utenti di Facebook si illudono se pensano di poter controllare le informazioni che forniscono a terze parti.

La privacy ha sempre riguardato la segretezza. Un imputato accusato di rivelare informazioni personali altrui poteva addurre in sua difesa il fatto che tali informazioni non fossero segrete. Ma, chiaramente, la questione della privacy è un po' più complicata. Solo perché comunichiamo certe cose alla nostra compagnia di assicurazioni non vuol dire che non ci sentiamo violati quando tali informazioni vengono vendute a un data broker. Solo perché raccontiamo un segreto a un nostro amico non significa che ci faccia piacere che lui lo racconti ad altri. Stesso dicasi per il nostro datore di lavoro, la nostra banca, o qualsiasi altra azienda con la quale ci rapportiamo.

Ma come dimostra l'esempio di Facebook, la privacy è una questione molto più complessa. Riguarda la nostra scelta di fornire informazioni a chi, come e per quale motivo. E la parola chiave qui è "scelta". Le persone sono portate a condividere ogni genere di informazione, purché ne mantengano il controllo.

Quando Facebook ha unilateralmente cambiato le regole su come venivano rivelate le informazioni personali, ha ricordato agli utenti che non erano loro ad avere il controllo. Gli otto milioni di membri hanno inserito le proprie informazioni nel sito basandosi su un insieme di regole che riguardavano l'uso di quei dati. Non c'è da stupirsi se tali membri (ragazzi della scuola superiore e del college, a cui tradizionalmente poco importa della propria privacy) si siano sentiti violati quando Facebook ha modificato le regole.

Purtroppo Facebook può cambiare le carte in tavola quando e come vuole. La sua Policy sulla Privacy è lunga 2.800 parole, e si conclude con una nota che avverte che può essere modificata in qualsiasi momento. Quanti utenti hanno mai letto tale policy, quanti l'hanno letta regolarmente a caccia di eventuali modifiche? Non che una Policy sulla Privacy sia la stessa cosa di un contratto. Da un punto di vista legale, Facebook possiede tutti i dati che i membri caricano sul sito. Può vendere quei dati a inserzionisti, marketer e data broker. (Nota: non vi è alcuna

prova che Facebook faccia tutto questo). Può permettere alla polizia di effettuare ricerche nei database, se richiesto. Può aggiungere nuove funzioni che cambiano chi e come può avere accesso a quali dati personali.

Ma la percezione del pubblico è importante. Qui la lezione per Facebook e altre aziende (come Google, MySpace, AOL e tutti coloro che offrono spazio web per le nostre email, i nostri siti, le nostre sessioni di chat) è che le persone credono di possedere i propri dati. Anche se la licenza d'uso può tecnicamente dare alle aziende il diritto di vendere quei dati, noi, gli utenti, la pensiamo diversamente. E quando noi, subìte le conseguenze di tali azioni, cominciamo a esprimere il nostro parere, sono guai.

Quel che Facebook avrebbe dovuto fare era aggiungere la nuova funzione come un'opzione, e permettere ai membri di scegliere di attivarla o meno. In questo modo, i membri interessati a condividere le proprie informazioni attraverso News Feeds avrebbero potuto farlo, e tutti gli altri non avrebbero avuto la sensazione di non avere voce in capitolo. Questa è certamente una zona grigia, ed è difficile sapere anticipatamente quali cambiamenti è necessario implementare con gradualità e quali non avranno pressoché alcun impatto. Facebook e altri devono comunicare apertamente con i propri membri quando varano nuove funzionalità. Ricordate: gli utenti vogliono il controllo.

La lezione per i membri di Facebook è forse ancora più stridente: se credono di avere il controllo sui propri dati, si stanno solo illudendo. Possono ribellarsi contro Facebook per aver cambiato le regole, ma le regole sono cambiate, a prescindere da ciò che fa l'azienda.

Ogni volta che si inseriscono dati in un computer, si perde parte del controllo su di essi. E quando li si affida a Internet, si perde molto del controllo su di essi. News Feeds ha portato i membri di Facebook faccia a faccia con l'intera portata delle conseguenze dell'aver inserito le proprie informazioni personali su Facebook. La difficoltà di aggregare i dati di più amici in un'unica posizione era qualcosa solo accidentalmente legato all'interfaccia utente. E anche se Facebook eliminasse completamente News Feeds, una terza parte potrebbe scrivere con facilità un programma che faccia la stessa cosa. Facebook potrebbe cercare di bloccare quel programma, ma alla fine perderebbe questa battaglia tecnica.

Stiamo tuttora lottando con le implicazioni di Internet in materia di privacy, ma l'ago della bilancia si è spostato in favore di una maggiore apertura. Le informazioni digitali sono troppo facili da spostare, copiare, aggregare e visualizzare. Compagnie come Facebook devono rispettare le regole sociali dei propri siti, devono pensare con attenzione alle proprie impostazioni predefinite (hanno un impatto enorme sui costumi della privacy dell'universo della Rete) e devono dare agli utenti quanto più controllo possibile sulle loro informazioni personali.

Ma dobbiamo tener presente che molto di quel controllo è illusorio.

Questo articolo è originariamente apparso su Wired.com.

<http://www.wired.com/news/columns/0,71815-0.html>

<http://www.danah.org/papers/FacebookAndPrivacy.html>

<http://www.motherjones.com/interview/2006/09/facebook.html>

<http://www.nytimes.com/2006/09/10/fashion/10FACE.html?ei=5090&en=ccb86e3d53ca671f&ex=1315540800&adxnll=1&partner=rssuserland&emc=rss&adxnllx=1160759797-MRZvPT2RgJLviJ0Z11NuRQ> oppure <http://tinyurl.com/ycwl6o>

<http://www.thememoryhole.org/nsa/bibs.htm>

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

News

Ancora sullo scandalo Hewlett-Packard:

http://www.schneier.com/blog/archives/2006/09/more_on_the_hp.html

Il crimine cibernetico sta guadagnando posizioni nella catena alimentare criminale: viene coinvolto un numero sempre maggiore di associazioni del crimine organizzato.

<http://www.wired.com/news/wireservice/0,71793-0.html>

Sono anni che vado dicendo cose simili, ed è da molto tempo che lamento il fatto che il cyber-terrorismo attira su di sé tutta l'attenzione della stampa, mentre è il crimine cibernetico la vera minaccia. Non credo che questo articolo sia tutto paure e sensazionalismi: si tratta di un problema reale.

È possibile programmare una macchina bancomat per farle credere che i biglietti da 20 dollari siano biglietti da 5, per poi prelevare il quadruplo della cifra richiesta. In effetti è sorprendentemente facile.

http://www.schneier.com/blog/archives/2006/09/programming_atm.html

Chi richiede un visto per gli Stati Uniti deve rispondere, fra le altre, a questa domanda: "È mai stato arrestato o condannato per aver commesso un reato anche se ha beneficiato di condoni, amnistie o altri provvedimenti di legge similari? È mai stato trafficante di droga, ha mai praticato o favorito la prostituzione?"

E questa: "È sua intenzione recarsi negli USA per impegnarsi in azioni che violano le norme sull'esportazione oppure per azioni sovversive, terroristiche o comunque illegali? È membro o rappresentante di una organizzazione attualmente riconosciuta come terroristica dal Segretario degli Stati Uniti? Ha mai partecipato a persecuzioni sotto il controllo del governo Nazista tedesco o ha mai preso parte a un genocidio?"

http://www.schneier.com/blog/archives/2006/09/us_visa_applica.html

I tedeschi stanno controllando la spazzatura degli inglesi. Cose del genere non si possono inventare così su due piedi:

<http://www.thisislondon.co.uk/news/article-23364736-details/Spy+in+your+wheelie+bin/article.do> oppure <http://tinyurl.com/f9fx4>

Una nota anonima nello Harvard Law Review sostiene che gli attacchi Internet apportano vantaggi significativi:

http://www.harvardlawreview.org/issues/119/june06/note/immunizing_the_internet.pdf oppure <http://tinyurl.com/e7pkf>

È possibile aprire la portiera di un'auto con sole 3.129 pressioni di una serie di tasti. In media, la metà dovrebbero bastare. (L'articolo è del 2004).

http://everything2.com/index.pl?node_id=1520430

Torpark è un browser web anonimo e gratuito. Si basa su una versione portatile di Firefox, gira anche su una chiavetta USB per cui non lascia tracce sul PC, e fa uso del network TOR per la navigazione web anonima.

http://www.darkreading.com/document.asp?doc_id=104381

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

http://www.boingboing.net/2006/09/19/torpark_is_out_offer.html

Divertente storia dal futuro: "Tecnico Diebold 19enne vince le elezioni presidenziali americane".

<http://www.avantnews.com/modules/news/article.php?storyid=281>

Calamari "steganografici" che possono celare dei messaggi nella propria pelle:

<http://www.sciencedaily.com/releases/2006/09/060920191616.htm>

The Onion sul divieto imposto dalla TSA sui liquidi:

http://www.theonion.com/content/node/53536?utm_source=onion_rss_daily

Un nuovo e intelligente protocollo di voto proposto da Ron Rivest:

<http://theory.csail.mit.edu/~rivest/Rivest-TheThreeBallotVotingSystem.pdf> oppure <http://tinyurl.com/hrjmq>

Storia interessante sui rischi di morire senza comunicare a nessuno le password del proprio computer.

http://news.com.com/Taking+passwords+to+the+grave/2100-1025_3-6118314.html oppure <http://tinyurl.com/gfdzh>

Pauroso falso allarme di sicurezza aerea. Ecco che cos'è il vigilantismo:

http://www.schneier.com/blog/archives/2006/10/this_is_what_vi.html

Finta vulnerabilità nel JavaScript di Firefox:

http://www.schneier.com/blog/archives/2006/10/firefox_javascript.html

Un post davvero interessante su un tizio che ha scoperto vulnerabilità SQL injection con Google. Secondo i suoi risultati, l'11,3% dei siti web è vulnerabile a questo tipo di attacco.

http://portal.spidynamics.com/blogs/msutton/archive/2006/09/26/How-Prevalent-Are-SQL-Injection-Vulnerabilities_3F00_.aspx oppure <http://tinyurl.com/lw98p>

"PhishTank è un'organizzazione d'équipe per la raccolta di dati e informazioni sul phishing in Internet. PhishTank inoltre fornisce una API aperta a sviluppatori e ricercatori per integrare liberamente i dati anti-phishing nelle loro applicazioni".

<http://www.phishtank.com>

60 Minutes ha ottenuto una copia della no-fly list della TSA. Gli errori e i problemi sono enormi.

<http://rawstory.com/showoutarticle.php?src=http%3A%2F%2Fwww.cbsnews.com%2Fstories%2F2006%2F10%2F05%2F60minutes%2Fmain2066624.shtml> oppure <http://tinyurl.com/ymc6ov>

Il Dipartimento per la Sicurezza Nazionale sta finanziando lo sviluppo di un software per monitorare le opinioni contenute nei quotidiani in tutto il mondo. Si può facilmente immaginare l'agghiacciante effetto che una cosa del genere potrà avere sulla libertà di stampa a livello mondiale.

http://www.schneier.com/blog/archives/2006/10/opinion_monitor.html

Si può utilizzare la nuova funzione di ricerca di codice offerta da Google per trovare nomi utente e password, codice confidenziale, buffer overflow, e ogni genere di altre cose.

<http://www.kottke.org/06/10/google-code-search>

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9003938&source=NLT_SEC&nid=38 oppure

<http://tinyurl.com/zg5ae>

http://monkey.org/~jose/blog/viewpage.php?page=google_code_search_stats

>

La sicurezza aeroportuale ha confiscato una roccia.

http://www.courant.com/news/opinion/op_ed/hc-thorson1005.artoct05,0,777

555.column?coll=hc-headlines-oped>

oppure <http://tinyurl.com/zkz43>>

Già sequestrano forbici. Quanto manca prima che si mettano a confiscare la carta?

La continua paranoia per il terrorismo è alla base di un'ennesima vicenda ridicola: una squadra HAZMAT viene chiamata per rimuovere un ammasso di gelatina di frutta lasciato ai margini di una strada.

<http://news.bbc.co.uk/1/hi/world/europe/6035821.stm>

Nel tentativo di risolvere il problema degli impostori in false uniformi, la polizia irachena ora possiede un'uniforme che è molto più difficile da imitare. Sarà certamente d'aiuto, ma non vedo che differenza può fare per il comune cittadino quando qualcuno vestito da poliziotto irrompe nella sua abitazione durante la notte. O quando dei terroristi in uniforme di polizia assassinano il fratello del vicepresidente iracheno Tariq al-Hashimi.

<http://english.aljazeera.net/NR/exeres/A1853C26-1620-4BE4-A819-4BF569B9394A.htm>> oppure <http://tinyurl.com/ykr4nl>>

http://www.swissinfo.org/eng/international/ticker/detail/Gunmen_kill_br

[other_of_Iraq_s_VP.html?siteSect=143&sid=7143598&cKey=1160413744000](http://www.swissinfo.org/eng/international/ticker/detail/Gunmen_kill_br_other_of_Iraq_s_VP.html?siteSect=143&sid=7143598&cKey=1160413744000)> oppure <http://tinyurl.com/s97qp>>

Fukuyama sulla segretezza:

http://www.nytimes.com/2006/10/08/books/review/Fukuyama.t.html?_r=1&bu&emc=bu&oref=slogin> oppure <http://tinyurl.com/y52t5m>>

Bell'articolo sull'idiozia della teoria della tortura "ticking time bomb":

<http://balkin.blogspot.com/2006/10/torture-and-ticking-time-bomb.html>>

Si veda anche:

<http://fafblog.blogspot.com/2005/03/would-you-could-you-in-box-theres-bomb.html>> oppure <http://tinyurl.com/ybsnzf>>

Non male come idea stupida: etichettare tutti i passeggeri negli aeroporti.

<http://news.bbc.co.uk/1/hi/technology/6044310.stm>

http://www.theregister.co.uk/2006/10/12/airport_rfid/>

La Rand Corporation pubblicò "A Million Random Digits with 100,000 Normal Deviates" nel lontano 1955, quando la generazione di numeri casuali era tutt'altro che semplice. Ho una copia dell'edizione originale: è uno dei pezzi più pregiati della mia biblioteca. Non sapevo che il libro è stato ristampato nel 2002: è disponibile su Amazon. Anche se non siete intenzionati ad acquistarlo, andate alla pagina web di Amazon e leggete le recensioni degli utenti. Sono divertentissime.

http://www.amazon.com/Million-Random-Digits-Normal-Deviates/dp/0833030477/sr=8-1/qid=1160657548/ref=pd_bbs_1/102-7977781-1757709?ie=UTF8>

http://www.schneier.com/blog/archives/2006/10/a_million_rando.html>

** *** *****

Il pupillometro

Questo dispositivo EyeCheck ha tutte le caratteristiche per sembrare un prodotto-burla: "Il dispositivo ha l'aspetto di un binocolo, e nel giro di pochi secondi effettua una scansione delle pupille del soggetto per rilevare eventuali problemi.

"Tale dispositivo sarà in grado di stabilire se il soggetto si trova sotto l'effetto di droghe, e di quale tipo di droga: marijuana, cocaina,

alcool. E nel caso del conducente di un trattore a rimorchio, l'apparecchio può stabilire se il soggetto è troppo stanco per guidare" ha detto Tom Burgoyne, sceriffo della contea dell'Ohio.

"Il dispositivo può inoltre rilevare anomalie derivate da effetti chimici e biologici, nonché disastri naturali".

L'apparecchio viene chiamato pupillometro e, secondo il sito web della compagnia, "si serve di tecnologie brevettate per produrre misurazioni affidabili della pupilla in meno di cinque minuti allo scopo di rilevare stanchezza o uso di droghe". E malgrado le implicazioni dell'articolo, il dispositivo non effettua tali rilevamenti a distanza.

La ricerca non mi lascia particolarmente impressionato, ma non ho competenza in questo campo.

<http://www.officer.com/article/article.jsp?id=32602&siteSection=1>
<http://www.mcjeyecheck.com/index.htm>
<http://www.mcjeyecheck.com/research.htm>

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

Piccoli display sulle smart card

Impressionante: un display che funziona su una carta di credito flessibile.

Uno dei maggiori problemi di sicurezza delle smart card è che non sono provviste di un proprio sistema di Input/Output. Ovvero, bisogna fare affidamento su qualsiasi lettore/scrittore di smart card perché invii ciò che scriviamo nella card e visualizzi la risposta. Nel 1999, Adam Shostack e il sottoscritto scrissero uno studio su questo problema di sicurezza di ordine generale.

Si pensi WYSIWTCs: What You See Is What The Card Says (Ciò che vedi è quel che dice la scheda): ecco il compito del display sulla smart card.

No, non è una protezione contro la manomissione della smart card. Questo fa parte di un insieme di minacce completamente diverso.

<http://www.cr80news.com/library/2006/09/16/on-card-displays-become-reality-making-cards-more-secure/> oppure <http://tinyurl.com/r7e6y>
<http://www.schneier.com/paper-smart-card-threats.html>

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

Cellulari che strillano

Da Wired:

"Vale la pena strillare se vi rubano il cellulare? Synchronica, un'azienda di gestione di dispositivi mobili, la pensa così. Se fate uso del servizio Mobile Manager della compagnia e vi viene sottratto il telefono, l'azienda, una volta contattata, bloccherà il cellulare a distanza, ne cancellerà tutti i dati e invierà un segnale per innescare un grido agghiacciante per spaventare il ladro".

La categoria generale di questo genere di misura di sicurezza si chiama "benefit denial" (lett. negazione del beneficio). Come quelle etichette

di plastica pinzate su capi di abbigliamento costosi: se li rubate e cercate di rimuovere l'etichetta, dell'inchiostro indelebile viene spruzzato sui vestiti e li rende inutilizzabili. L'efficacia di questo tipo di contromisura si affida al fatto che il ladro è al corrente della presenza (o della probabile presenza) di tale contromisura. È un deterrente piuttosto efficace contro il taccheggio; a mio parere una simile misura risulterà meno valida contro i ladri di cellulari.

La cancellazione a distanza dei dati contenuti in cellulari rubati, però, rimane comunque un'ottima idea. E dato che i telefoni cellulari vengono più spesso perduti che rubati, perché non fare in modo che il telefono annunci tranquillamente che è stato perduto e che vorrebbe essere riconsegnato al suo proprietario?

http://blog.wired.com/gadgets/index.blog?entry_id=1558434

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

Le news di Counterpane

L'Associated Press ha stilato un profilo su di me:
<http://apnews.excite.com/article/20060925/D8KBIJ480.html>

Il mese scorso ho tenuto una lezione sul tema "Il futuro della privacy" alla University of Southern California. La traccia audio è online.
http://uscpublicdiplomacy.org/index.php/events/events_detail/1925/

Schneier interverrà alla InfoSecurity Conference a Chicago il 20 ottobre:
<http://infosecurityconference.techtarget.com/>

Schneier interverrà alla RSA Europe a Nizza, in Francia, il 24 ottobre:
<http://2006.rsaconference.com/europe/>

Schneier interverrà al Rendez-vous de la Securite de l'Information a Montreal il 30 ottobre:
<http://rsec-info.com/>

Schneier interverrà alla ACLU Delaware Membership Conference a Wilmington il 10 novembre:
<http://www.aclu-de.org/Paranoid%20Society%20Conference.htm>

Schneier interverrà alla ACLU Rhode Island a Providence il 16 novembre:
<http://www.riaclu.org/events.html>

Counterpane ha annunciato nuove soluzioni di sicurezza dei dati che supportano piattaforme IBM, SAP, Oracle e MSSQL, per aiutare i clienti a difendersi contro attività non autorizzate e per migliorare la conformità.

<http://www.counterpane.com/pr-20061009.html>
<http://www.counterpane.com/pr-20061002.html>
<http://www.counterpane.com/pr-20060918.html>

Le attuali offerte di lavoro di Counterpane:
<http://www.counterpane.com/jobs.html>

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

Novità su FairUse4WM

Un paio di settimane fa ho parlato della battaglia fra il sistema DRM di Microsoft e FairUse4WM, che lo compromette. Le ultime novità sono che Microsoft ha emesso una patch contro FairUse4WM 1.2 e ha intentato una causa legale contro gli autori anonimi del programma; la risposta di tali autori è stata rilasciare FairUse4WM 1.3, che rompe la patch Microsoft più recente.

Da Engaget: "Abbiamo chiesto a Viodentia in merito alle accuse dell'azienda di Redmond secondo cui lui e/o i suoi associati sono penetrati nei sistemi [di Microsoft] così da ottenere l'IP necessario per craccare PlayForSure; Vio ha dichiarato di essere 'profondamente scosso' dalle accuse. 'Non ho utilizzato alcun codice sorgente Microsoft. Ma credo che questa causa non sia altro che una battuta di caccia per ottenere informazioni di identità che possono poi essere utilizzate per intentare cause più mirate, o per provocare altri guai'. Siamo certi che a Microsoft farebbe piacere che i propri partner e l'opinione pubblica pensassero che il suo DRM sia generalmente infallibile e che sia necessario rubare il suo IP per craccarlo, pertanto la conclusione di Viodentia sulle tattiche legali di Microsoft ci sembra attendibile, ovvia e del tutto logica".

La cosa interessante di questa saga tuttora in corso è come essa sia diversa dalla solita sequenza per cui si scopre una vulnerabilità e si rilascia una patch. Gli autori di FairUse4WM non stanno cercando dei bug per scoprire come sfruttarli, costringendo Microsoft a emettere delle patch. È invece una sequenza di cracking, patch, ri-cracking, ri-patch, e così via.

Il motivo per cui stiamo assistendo a tutto questo (e ciò diventerà la norma per i sistemi DRM) è che il DRM è fondamentalmente un problema impossibile. Per farlo funzionare già sono necessari degli espedienti, e il compromettere, il distruggere il DRM è qualcosa di più simile a "sistemare" il software, in modo che tali espedienti non possano funzionare. Chiunque voglia una dimostrazione che il destino del DRM tecnico è segnato, dovrebbe seguire gli sviluppi di questa vicenda. (Se Microsoft ha qualche possibilità di vittoria, è solo sul piano legale).

http://www.schneier.com/blog/archives/2006/09/microsoft_and_f.html
<<http://www.engadget.com/2006/09/25/microsoft-claims-successful-patch-against-fairuse4wm-1-2/>> oppure <<http://tinyurl.com/rndpv>>
<<http://arstechnica.com/news.ars/post/20060927-7849.html>>
<<http://www.engadget.com/2006/09/27/viodentia-responds-to-microsoft-releases-fairuse4wm-1-3/>> oppure <<http://tinyurl.com/p3osv>>

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

Software per il voto elettronico e segretezza

Ecco una dichiarazione di un funzionario elettorale di Los Angeles: "Il software sviluppato per InkaVote è software proprietario. Tutto il software sviluppato dai vari produttori è proprietario. Trovo strano che certa gente non voglia che sia proprietario. Se si mette a disposizione il codice open source, si renderebbero pubbliche anche le indicazioni per violare il software. Noi crediamo che la natura proprietaria del software sia un'ottima cosa per la sicurezza".

È tutto molto buffo, davvero. Ciò che intendeva questa persona, e che avrebbe dovuto dire, è una cosa del genere: "Trovo strano che chiunque abbia esperienza in sicurezza informatica non voglia che il software sia proprietario. Parlando da completa ignorante in materia di sicurezza

informatica, ritengo che la segretezza sia una risorsa". Questa è una dichiarazione più realistica.

Come ho già detto e ripetuto, la segretezza è diversa dalla sicurezza, non è la stessa cosa. E in molti casi la segretezza non è altro che un danno per la sicurezza.

http://www.dailynews.com/news/ci_4407865?source=email

Segretezza e sicurezza:

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

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

La legge sulla tortura in forma di codice C

Kevin Poulsen riassume la nuova legge sull'arresto/reclusione/tortura di terroristi (e altri) in un breve frammento di codice C:

```
if (person = terrorist) {
punish_severely();
} else {
exit(-1);
}
```

Vi è un errore macroscopico, ma vi sono anche altri problemi con questo codice. Qualcuno vuole commentare in proposito?

http://blog.wired.com/27bstroke6/2006/09/bad_code.html

http://www.boingboing.net/2006/10/02/the_us_torture_bill_.html

http://www.schneier.com/blog/archives/2006/10/torture_bill_as.html

La legge statunitense:

<http://thomas.loc.gov/cgi-bin/query/z?c109:S.3930.ES:>>

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

Il Canile: SecureRF

SecureRF: "Dichiara di fornire una prima sicurezza veramente realizzabile per i RFID. La crittografia a chiave pubblica tradizionale (come la RSA) è troppo intensiva per un RFID da un punto di vista computazionale. SecureRF mette a disposizione una tecnologia simile ma con un ingombro estremamente inferiore sfruttando un'area piuttosto oscura della matematica: la teoria dei gruppi infiniti, che deriva fra l'altro dalla teoria dei nodi, una branca della topologia".

Nel loro sito web sostengono di avere i "libri bianchi" sulla teoria, ma per averli dovete inserire informazioni personali. Naturalmente non viene fatto alcun riferimento a veri e propri studi crittografici già pubblicati. La "nuova matematica" è il mio Segnale d'Allarme Snake-Oil n. 2, e ho il forte sospetto che la loro documentazione contenga altri analoghi segnali di allarme. Io starei alla larga da questa gente.

http://www.oreillynet.com/etel/blog/2006/09/embedded_systems_conference_20.html

oppure <http://tinyurl.com/yz9e2k>

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

Segnali d'allarme Snake-oil:

<http://www.schneier.com/crypto-gram-9902.html#snakeoil>

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

Hacking ai danni del Bureau of Industry and Security

Il BIS (Bureau of Industry and Security) è la sezione del Dipartimento del Commercio USA responsabile del controllo sulle esportazioni. Se si possiede una tecnologia a doppio uso per la quale è necessaria un'autorizzazione speciale per l'esportazione al di fuori degli Stati Uniti, o per l'esportazione verso determinati paesi, è il BIS l'ente a cui si deve fare riferimento e a cui inoltrare la documentazione.

È stato penetrato da "hacker che hanno agito attraverso server cinesi", ed è stato chiuso. Potrebbe anche essere stato un attacco mirato.

I costruttori di dispositivi hardware crittografici (escluso il software che è prodotto seriale di massa) devono inviare informazioni progettuali dettagliate al BIS per ottenere una licenza di esportazione. Nei computer del BIS vi è una grande quantità di dati sui prodotti crittografici.

Naturalmente non mi è possibile sapere se queste informazioni sono state rubate o se erano quel che stavano cercando gli hacker, ma la faccenda è interessante. D'altro canto, qualsiasi prodotto crittografico che si affidava alla segretezza di tali informazioni non merita comunque di essere sul mercato.

<<http://www.techweb.com/showArticle.jhtml;jsessionid=OM4E5LCHY4W0WQSNDLRCKHSCJUNN2JVN?articleID=193105174>>
oppure <<http://tinyurl.com/epsq2>>

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

Le reti universitarie e la sicurezza dei dati

In generale, i problemi legati alla protezione di una rete universitaria non sono molto diversi da quelli legati alla protezione di una qualsiasi grande rete aziendale. Ma per quanto riguarda la sicurezza dei dati, le università presentano problematiche specifiche. È facile puntare il dito contro gli studenti, che rappresentano una grande quantità di membri interni di passaggio potenzialmente ostili. Allo stesso tempo non è una situazione molto differente da quella di una multinazionale che ha a che fare con una grande varietà di impiegati e fornitori. La differenza sta nella cultura.

Le università si concentrano sui margini: le politiche centrali sono tendenzialmente e intenzionalmente deboli, e viene concessa la massima autonomia ai margini, alla periferia. Ciò significa che le università hanno la tendenza naturale a opporsi alla centralizzazione dei servizi. Interi dipartimenti e singoli professori sono abituati a essere semi-indipendenti. Dato che queste istituzioni sono state costituite molto prima dell'avvento dei computer, quando il networking ha iniziato a espandersi nelle università, si è sviluppato all'interno di divisioni amministrative già esistenti. Alcune università hanno dipartimenti accademici dotati di propri dipartimenti IT, di un proprio budget e di un proprio personale, con un gruppo IT centralizzato che fornisce la banda di rete e quasi nessuna supervisione. Purtroppo questi sottogruppi IT non annoverano fra le proprie competenze di base lo sviluppo e il

rispetto di linee di condotta.

La mancanza di un'autorità centrale rende assai complesso (per usare un eufemismo) far rispettare standard uniformi. Moltissimi CIO universitari hanno molto meno potere dei loro equivalenti aziendali; i mandati universitari possono rappresentare un grosso ostacolo per l'imposizione di qualsiasi policy di sicurezza. Questo porta a un panorama di sicurezza fortemente disomogeneo.

Da parte delle facoltà e del personale vi è poi una tendenza di tipo culturale all'opposizione alle restrizioni, specialmente nel campo della ricerca. Dato che molta della ricerca oggi viene svolta online (o, almeno, prevede l'accesso online), limitare l'utilizzo o decidere gli usi appropriati delle tecnologie di informazione può essere arduo. Questa resistenza inoltre porta a una mancanza di centralizzazione e all'assenza di procedure operative IT quali controllo del cambiamento, gestione del cambiamento, gestione delle versioni e gestione della configurazione.

Il risultato è che raramente si può trovare una policy di sicurezza omogenea. I server centralizzati (il nucleo dove risiedono i server database) sono generalmente più sicuri, mentre la periferia è un guazzabuglio di livelli di sicurezza.

Che cosa fare, quindi? Sfortunatamente le soluzioni sono più facili da descrivere che da mettere in pratica. Anzitutto le università dovrebbero considerare un approccio dall'alto verso il basso nella protezione della propria infrastruttura. Piuttosto che combattere una cultura già costituita, dovrebbero concentrarsi sulla core infrastructure.

Poi dovrebbero spostare i dati personali, finanziari e altre informazioni paragonabili all'interno di quel core. Ai dipartimenti e ai gruppi di ricerca si lascino le informazioni importanti di loro pertinenza, e si conservino centralmente quei dati che sono importanti per l'intera università. Questo può essere fatto sotto gli auspici del CIO. Leggi e normative possono contribuire al consolidamento e alla standardizzazione.

In seguito, imporre delle policy per quei dipartimenti che necessitano l'accesso ai dati sensibili della core infrastructure. Ciò può essere difficile da attuare in presenza di sistemi ormai datati, ma stabilire uno standard di buone pratiche è sicuramente meglio che lasciar perdere. Tutta la vecchia tecnologia prima o poi viene aggiornata.

Infine, creare sottoreti distinte e isolate all'interno del campus. Trattare tutte le reti che non sono sotto il diretto controllo del dipartimento IT come reti non fidate. Le reti degli studenti, per esempio, dovrebbero essere disposte dietro firewall per proteggere il nucleo centrale da esse. L'università può quindi stabilire livelli di fiducia in proporzione al rispetto delle policy da parte delle varie reti isolate. Se una rete di ricerca sostiene di non poter avere alcun controllo, allora l'università può metterle a disposizione una rete virtuale, fuori dai firewall universitari, e permetterle di operare in quell'ambito. Si noti, tuttavia, che se qualcosa o qualcuno su quella rete vuole collegarsi a dati sensibili all'interno del core, dovrà rispettare qualunque policy di sicurezza richiesta da tale livello di accesso dati.

Proteggere le reti universitarie è un ottimo esempio di come i problemi sociali intorno alla sicurezza di rete siano più complessi da risolvere di quelli tecnici. Ma complesso non significa impossibile, e si possono fare molte cose per migliorare la sicurezza.

Questo articolo è originariamente apparso sul numero di settembre/ottobre di IEEE Security & Privacy.

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

Commenti dei lettori

Su questi argomenti vi sono centinaia di commenti nel mio blog, molti davvero interessanti. Cercate l'argomento sul 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 sempre <http://www.schneier.com/crypto-gram.html>

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

I commenti a CRYPTO-GRAM devono essere inviati a schneier@counterpane.com. Si sottintende il permesso di riprodurre tali commenti, salvo indicazione contraria. I commenti possono venire adattati per ragioni di spazio e di chiarezza.

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 è leader mondiale nella protezione delle informazioni su network - l'inventore del Managed Security Monitoring gestito in outsourcing e la principale autorità nella riduzione efficace delle nuove minacce in ambito IT. Counterpane protegge reti per conto di governi e di aziende inserite nella Fortune 1000 a livello mondiale.

<http://www.counterpane.com>

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.