

CRYPTO-GRAM
15 novembre 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:

La sicurezza dei passaporti RFID
Le vulnerabilità dei software e le responsabilità
Le ristampe di Crypto-Gram
Prevenire il furto d'identità: i vivi e i morti
Le banche e l'autenticazione a due fattori
News
Sony installa di nascosto un rootkit sui computer
Revisione periodica del DMCA
Le News di Counterpane
Taser Cam
Un "tipico" terrorista
Il worm Zotob

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

La sicurezza dei passaporti RFID

Nel 2004, quando il Dipartimento di Stato USA iniziò a parlare della possibilità di incorporare chip RFID nei passaporti, vi fu grande clamore da parte dei sostenitori della privacy. Quando il Dipartimento di Stato pubblicò in febbraio una bozza del regolamento, ricevette 2.335 commenti, il 98,5% negativi. In risposta, le normative finali del Dipartimento di Stato, pubblicate il mese scorso, contengono due caratteristiche che tentano di affrontare le problematiche legate alla sicurezza e alla privacy. Ma permane un grave problema.

Prima di descrivere tale problema, può essere utile contestualizzare la polemica sull'argomento. I chip RFID sono passivi, e trasmettono informazioni a qualsiasi lettore che interroga il chip. Perciò i critici, me compreso, erano inizialmente preoccupati che i nuovi passaporti potessero rivelare la nostra identità senza il nostro consenso o addirittura a nostra insaputa. I ladri potrebbero raccogliere i dati sensibili delle persone mentre queste camminano per strada, i criminali potrebbero scansionare passaporti alla ricerca di ricchi

occidentali da sequestrare o da derubare, e i terroristi potrebbero innescare bombe in modo da esplodere solo quando, per esempio, quattro cittadini americani si trovano nei paraggi. La polizia potrebbe utilizzare i chip per sorvegliare un individuo; i centri commerciali potrebbero servirsi di questa tecnologia per identificare i clienti a loro insaputa.

I problemi di privacy dello RFID sono maggiori di quelli di passaporti e carte d'identità. L'industria dello RFID immagina un futuro in cui tali chip vengano incorporati ovunque: negli oggetti che acquistiamo, per esempio. Ma anche un chip che contenesse soltanto un unico numero di serie potrebbe essere usato a scopo di sorveglianza. Ed è semplice collegare il numero di serie a un'identità (per esempio quando si compra l'oggetto con una carta di credito) e da quel momento in poi identificarci. Data broker come ChoicePoint manterranno sicuramente dei database di numeri RFID e delle persone ad essi associate; si tratterebbe di un disservizio per i loro azionisti se non lo facessero.

Il Dipartimento di Stato ha minimizzato tali rischi insistendo sul fatto che i chip RFID funzionano solo a brevi distanze. Infatti, nella pubblicazione dello scorso mese si dichiara: "La tecnologia di prossimità utilizzata nel passaporto elettronico è progettata per essere letta da appositi lettori nei punti di ingresso solamente quando il documento viene disposto a pochi centimetri da tali lettori". Il problema è che si fa confusione su tre cose: la distanza alla quale il chip è progettato per essere letto, la distanza massima alla quale è possibile leggere il chip, e la distanza di intercettazione ovvero la distanza massima alla quale è possibile leggere il chip con una strumentazione specializzata. La prima è davvero di qualche centimetro, ma è stato dimostrato quest'anno che la seconda è di 69 piedi (21 metri abbondanti). La terza è di gran lunga maggiore.

E ricordiamoci che la tecnologia migliora sempre, non fa mai passi indietro. È semplicemente folle ritenere che queste distanze non aumenteranno col tempo.

A suo merito, va detto che il Dipartimento di Stato ha preso atto delle critiche. Come risultato, i passaporti RFID ora sono provvisti di una sottile schermatura radio incorporata nella custodia, che protegge il chip quando il passaporto rimane chiuso. Anche se alcuni hanno deriso questa soluzione, paragonandola a un involucro di carta stagnola per passaporti, tale contromisura impedirà che i documenti siano intercettati quando non sono in uso, cioè da chiusi.

Tuttavia, chiunque viaggi sa che i passaporti non vengono utilizzati solo per oltrepassare le frontiere. Spesso occorre mostrare il proprio passaporto negli alberghi e negli aeroporti, e quando si cambia del denaro. Sta diventando sempre più una carta d'identità; secondo nuove normative italiane, gli stranieri devono presentare il proprio passaporto prima di usufruire del servizio in un Internet café.

Per questo il Dipartimento di Stato ha aggiunto una seconda e più importante funzionalità: il controllo degli accessi. I dati nel chip saranno criptati, e la chiave stampata sul passaporto. Un ufficiale di frontiera farà passare il passaporto attraverso un lettore ottico per ottenere la chiave, quindi il lettore RFID si servirà della chiave per comunicare con il chip RFID.

Ciò significa che il possessore del passaporto può controllare chi ha accesso alle informazioni sul chip, e nessuno può sottrarre informazioni dal passaporto senza prima aprirlo e leggere i dati in esso contenuti. Ciò significa inoltre che una terza persona non può intercettare la comunicazione fra la scheda e il lettore, perché è criptata.

Queste funzionalità sono davvero esemplari, e dovrebbero servire da modello per qualsiasi applicazione RFID legata a documenti di identità. Purtroppo c'è ancora un problema.

I chip RFID, compresi quelli specifici per i passaporti statunitensi, possono ancora essere individualmente identificati grazie al loro comportamento radio. Nello specifico, questi chip possiedono un numero identificativo unico che viene utilizzato per evitare collisioni. È il sistema di cui si servono i chip per evitare problemi di comunicazione quando se ne dispongono molti accanto a un lettore. Si tratta di un particolare che si trova in profondità dentro al chip e non ha niente a che vedere con i dati o l'applicazione sul chip.

I costruttori di chip non amano parlare degli ID di collisione o di come funzionano, ma i ricercatori hanno dimostrato come identificare i singoli chip RFID interrogandoli e vedendo come si comportano. È dato che queste richieste accedono a un livello più profondo del chip che non l'applicazione passaporto, un meccanismo di controllo accessi non serve a molto.

Per ovviare a questo problema, il Dipartimento di Stato deve richiedere che i chip impiegati nei passaporti implementino un sistema di elusione delle collisioni non basato su numeri seriali unici. La specifica RFID (il cui nome è ISO 14443A) permette un sistema casuale, ma credo che nessun costruttore lo implementi in questo modo.

Aggiungere chip ai passaporti può indiscutibilmente essere una buona cosa per la sicurezza. La prima serie di chip conterrà soltanto le informazioni stampate sul passaporto, ma questo sistema ha da sempre previsto l'aggiunta di dati biometrici come fotografie o anche impronte digitali, che renderanno i passaporti più difficili da falsificare, e i passaporti rubati più difficili da utilizzare.

Ma l'opinione del Dipartimento di Stato, secondo cui i passaporti necessitano di chip RFID, perché i contact chip come quelli delle smartcard non funzioneranno, è assai meno convincente. Anche con tutta la sicurezza aggiunta, lo RFID dovrebbe essere l'ultima spiaggia delle scelte progettuali.

Il Dipartimento di Stato ha svolto un ottimo lavoro nell'affrontare le specifiche problematiche di sicurezza e privacy, ma la sua mancanza di preparazione tecnica sta rovinando tutto. La questione dell'elusione delle collisioni basata su numeri seriali è solo un esempio dell'impreparazione del Dipartimento di Stato, che gli ha impedito di impostare la cosa nel modo corretto.

Ovviamente può risolvere il problema, ma la vera questione è: quanti altri problemi come questo si nascondono nei dettagli del progetto? Non lo sappiamo, e dubito che il Dipartimento di Stato lo sappia. L'unico sistema per esaminare attentamente il suo progetto, e di convincerci che lo RFID è necessario, sarebbe quello di aprirlo ad un'analisi pubblica.

Il piano del Dipartimento di Stato di emettere passaporti RFID entro l'ottobre del 2006 è insieme precipitoso e rischioso. È stato un errore progettarlo a porte chiuse. Occorre che vi siano controlli di qualità e test molto accurati prima di mettere in opera questo sistema, e ciò comprende attente verifiche di sicurezza da parte di esperti di sicurezza indipendenti. Al momento il Dipartimento di Stato non ha alcuna intenzione di farlo: si è già impegnato su uno schema prima ancora di sapere se funzionerà o se proteggerà davvero la privacy.

L'annuncio governativo:

<http://edocket.access.gpo.gov/2005/05-21284.htm>

Problemi di privacy dello RFID:

<http://www.epic.org/privacy/rfid/>

<http://rfidkills.com/>

I miei passati interventi sui passaporti RFID:

<http://www.schneier.com/essay-060.html>

http://www.schneier.com/blog/archives/2005/04/rfid_passport_s.html

http://www.schneier.com/blog/archives/2005/08/rfid_passport_s_1.html

Questo articolo è apparso in precedenza su Wired.com:

<http://www.wired.com/news/privacy/0,1848,69453,00.html>

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

Le vulnerabilità dei software e le responsabilità

A una conferenza sulla sicurezza tenutasi il mese scorso, Howard Schmidt, ex-consigliere sulla sicurezza cibernetica alla Casa Bianca, ha coraggiosamente sostenuto che gli sviluppatori di software dovrebbero essere resi personalmente responsabili della sicurezza del codice che scrivono.

Schmidt è sulla strada giusta, ma ha commesso un pericoloso errore. Sono i produttori di software che dovrebbero essere resi responsabili, non i singoli programmatori. Se si lavora a questa idea nel modo giusto, si otterrà software più sicuro per tutti; se l'approccio è sbagliato, il risultato sarà semplicemente una confusa sequela di cause giudiziarie.

Per comprendere la differenza, è necessario capire gli incentivi economici basilari delle aziende, e come le responsabilità agiscono sulle imprese. In una società capitalistica, le compagnie sono imprese che mirano al profitto, e le loro decisioni vengono prese in base a una redditività a breve e a lungo termine. Cercano di bilanciare i costi di un software più sicuro (più sviluppatori, meno funzionalità, tempistiche più lunghe per la commercializzazione) contro i costi di software non sicuro: spese per la realizzazione delle patch, un'occasionale pubblicità negativa, perdita potenziale delle vendite.

Il risultato lo vediamo tutti: software pessimo. Le aziende trovano che sia più economico resistere all'occasionale tempesta di pubblicità negativa, spendere soldi in campagne di pubbliche relazioni che vantano ottima sicurezza, e risolvere i problemi pubblici dopo il fatto, invece di progettare e considerare la sicurezza fin dall'inizio.

Il problema di quest'analisi è che la maggior parte dei costi del software insicuro ricadono sugli utenti. In economia questo fatto viene chiamato esternalità: l'effetto di una decisione non viene sostenuto da chi ha preso quella decisione.

Normalmente ci si aspetterebbe che gli utenti rispondessero favorendo i prodotti sicuri a scapito di quelli non sicuri: dopotutto stanno prendendo le loro decisioni di acquisto basandosi sullo stesso modello capitalistico. Ma ciò non è generalmente possibile. In alcuni casi, certi monopoli in ambito software limitano le scelte a disposizione nell'acquisto di un prodotto; in altri casi, l'effetto di "chiusura" creato da formati di file proprietari o da un'infrastruttura già esistente o da requisiti di compatibilità, rende più difficile il cambiamento; e in altri casi ancora, nessuna delle aziende concorrenti ha fatto della sicurezza un elemento di distinzione. In ogni caso, per

l'acquirente medio è difficile distinguere un prodotto veramente sicuro da un prodotto non sicuro ma con una campagna di marketing tutta mirata a decantarne la sicurezza.

Il risultato finale è la grande diffusione di software non sicuro. Ma dato che sono gli utenti a pagarne il prezzo, e non i produttori di software, non vi sono miglioramenti. Rendendo responsabili i produttori di software si rimedia a questa esternalità.

Si osservi il meccanismo in funzione. Se gli utenti finali possono denunciare i produttori di software per difetti presenti nei prodotti, allora il costo di quei difetti aumenterà per i produttori di software, che finiscono col pagare il reale costo economico del pessimo software, e non solo una parte di esso. Per cui, quando si tratta di bilanciare da una parte il costo per rendere sicuro il proprio software e dall'altra il costo di lasciarlo insicuro, i costi di quest'ultima saranno decisamente maggiori. Ciò fornirà un incentivo per rendere il software più sicuro.

Sicuramente, rendere il software più sicuro avrà i suoi costi, e i produttori dovranno passare quei costi agli utenti finali aumentando i prezzi. Ma gli utenti stanno già pagando i costi addizionali del software non sicuro: i costi per prodotti di sicurezza di terze parti, i costi delle consulenze e delle società che offrono servizi di sicurezza, i costi diretti e indiretti delle perdite. Rendere i produttori di software responsabili fa muovere maggiormente quei costi, e come prodotto secondario causa l'aumento in qualità del software.

Ecco perché l'idea di Schmidt non funzionerà. Egli vuole che siano responsabili i singoli sviluppatori di un software, e non le aziende. Ciò fornirà senza dubbio un capro espiatorio che gli utenti arrabbiati potranno denunciare, ma non ridurrà l'esternalità e non risulterà in un software più sicuro.

La sicurezza informatica non è un problema tecnologico, ma economico. I socialisti possono immaginare che le aziende miglioreranno la sicurezza dei programmi come spontaneo atto di buona volontà, ma i capitalisti sanno che ciò deve rientrare nel miglior interesse delle aziende. Avremo meno vulnerabilità quando chi ha la capacità di ridurre tali vulnerabilità avrà l'incentivo economico di farlo. Ed è per questo che soluzioni quali responsabilità e normative funzionano.

I commenti di Schmidt:

<http://news.zdnet.co.uk/software/developer/0,39020387,39228663,00.htm>

Il thread su SlashDot riguardante le problematiche sollevate da Schmidt: <http://developers.slashdot.org/article.pl?sid=05/10/12/1335215&tid=172&tid=8> oppure <http://tinyurl.com/dvdp7>

Dan Farber ha fornito un buon commento al mio articolo.

<http://blogs.zdnet.com/BTL/?p=2046>

Questo articolo è originariamente apparso su Wired.com:

<http://www.wired.com/news/privacy/0,1848,69247,00.html>

C'è stata un po' di confusione a riguardo nei commenti (sia su Wired che nel mio blog), e molti hanno pensato che ciò significhi che ci si aspetterà la perfezione da parte dei produttori di software e che saranno ritenuti responsabili al 100% se ciò non accadrà. Ovviamente una cosa del genere è ridicola e non è certo questo il modo in cui funzionano le responsabilità. Ma egualmente ridicolo è ritenere che i produttori di software dovrebbero essere del tutto esenti da responsabilità sui difetti. Una quantità ragionevole di responsabilità

<http://www.schneier.com/crypto-gram-0011.html#1>

Programmare il computer di Satana, ovvero: perché i computer non sono sicuri:

<http://www.schneier.com/crypto-gram-9911.html#WhyComputersareInsecure>
oppure <http://tinyurl.com/7ldrl>

La crittografia a chiave pubblica basata sulla matematica delle curve ellittiche (Elliptic Curve Cryptography):

<http://www.schneier.com/crypto-gram-9911.html#EllipticCurvePublic-KeyCryptography> oppure <http://tinyurl.com/a2low>

Il futuro della frode: tre motivi che spiegano perché il commercio elettronico è diverso.

<http://www.schneier.com/crypto-gram-9811.html#commerce>

La protezione anti-copia del software e perché non funziona:

<http://www.schneier.com/crypto-gram-9811.html#copy>

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

Prevenire il furto d'identità: i vivi e i morti

Una società chiamata Metacharge sta offrendo un servizio e-commerce di sicurezza nel Regno Unito. Per un costo di circa 2 dollari a nome, gli operatori del sito Web possono autenticare i loro clienti mettendo a confronto i nominativi con il Registro Elettorale Britannico, l'elenco telefonico British Telecom e un database di mortalità.

Non è a buon mercato, e la società mira in special modo a clienti in industrie ad alto rischio, come il gioco d'azzardo online. Ma l'economia che sta dietro a questo sistema è interessante da esaminare. Illustra le esternalità associate alla frode e al furto d'identità, e mostra come non si risolverà il problema lasciando le cose in mano alle aziende.

Il database di mortalità è interessante. Secondo Metacharge "il tipo di furto di identità che si sta diffondendo sempre più rapidamente non è il phishing, ma il rubare le identità di persone defunte e utilizzarle per ottenere un credito".

Per un sito Web, l'economia è semplice: costa 2 dollari verificare che un cliente sia vivo. Se la probabilità che un cliente sia in effetti defunto (e quindi fraudolento) moltiplicata per le perdite medie dovute a questo cliente defunto è maggiore di 2 dollari, allora il servizio ha senso. Se è minore, allora il servizio non ha senso. Per esempio, se i clienti defunti sono uno ogni diecimila, e ognuno costa 15.000 dollari, allora il servizio non vale la pena. Se costano 25.000 dollari l'uno, o se il tasso di frequenza è doppio, allora vale la pena.

Adesso immaginiamo che vi sia un servizio analogo che individui la frode di identità fra persone viventi. La medesima analisi economica continuerebbe a valere. Ma in questo caso abbiamo una esternalità: un costo aggiuntivo di frode sostenuto dalla vittima e non dal sito Web. Per cui, se una frode effettuata usando l'identità di clienti vivi avvenisse con un tasso di frequenza di uno ogni diecimila, e ogni caso costasse 15.000 dollari al sito Web e altri 10.000 dollari alla vittima, il sito Web concluderebbe che il servizio non vale la pena, anche se pagare per esso è in generale meno costoso. Ecco perché occorre una legge che innalzi il costo delle frodi per i siti Web.

C'è un altro compromesso economico. I siti Web hanno due principali

opportunità per autenticare i clienti che usano servizi come questi. La prima è quando registrano il cliente, e la seconda è in seguito a una qualsiasi forma di non-pagamento. Molti dei danni al cliente avvengono dopo che il non-pagamento viene riferito a un'agenzia di credito, per cui avrebbe senso effettuare qualche controllo di identificazione in più, a quel punto. Al sito Web verrebbe a costare certamente meno, a condizione che venga pagato un minor numero di controlli. Ma dato che la seconda opportunità accade dopo che il sito Web ha accusato le perdite, non ha alcun incentivo ad approfittarne. Ancora una volta, è l'economia a guidare la sicurezza.

http://www.theregister.co.uk/2005/10/21/outlaw_gambling/

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

Le banche e l'autenticazione a due fattori

Ho più volte sostenuto come l'autenticazione a due fattori non fermerà il phishing, poiché gli aggressori non faranno altro che modificare le loro tecniche per aggirarla. Ecco un esempio in cui è accaduto proprio questo:

"La banca scandinava Nordea è stata costretta a chiudere una parte del suo servizio di Web banking per 12 ore la scorsa settimana a seguito di un attacco di phishing specificamente mirato al suo sistema di sicurezza cartaceo basato su password usa-e-getta.

"Secondo quanto riportato dalla stampa, la truffa ha preso di mira i clienti che accedono al sito di Web banking di Nordea usando un sistema di sicurezza basato su password da utilizzarsi una sola volta, stampate su carta.

"Un'entrata del blog dell'azienda finlandese di sicurezza F-Secure dice che i destinatari della falsa email venivano reindirizzati verso siti fasulli, e inoltre veniva loro chiesto di inserire i dettagli del loro account, unitamente alla prossima password presente nella lista di password da usarsi una sola volta stampata dalla banca".

Dal blog di F-Secure:

"Le email fasulle spiegavano che Nordea sta introducendo nuove misure di sicurezza, visibili agli indirizzi www.nordea-se.com o www.nordea-bank.net (siti fasulli ospitati nella Corea del Sud).

"I siti falsi apparivano abbastanza veritieri. Richiedevano all'utente il suo numero personale, il codice di accesso, e il prossimo codice usa-e-getta valido. A prescindere da ciò che si scriveva, il sito lamentava l'inesattezza del codice usa-e-getta e chiedeva di provare a inserire il seguente. In realtà era un tentativo degli aggressori di raccogliere quanti più codici possibili e usarli per transazioni personali."

L'autenticazione a due fattori non fermerà il furto d'identità, perché esso non è un problema di autenticazione: si tratta di un problema di sicurezza della transazione. Ho già scritto a riguardo. Le soluzioni al problema dovranno affrontare direttamente le transazioni, e ritengo che si tratterà di una combinazione di elementi. Alcune transazioni diventeranno più scomode. Diventerà certamente più complicato ottenere una nuova carta di credito. Verranno implementati sistemi back-end per identificare pattern di transazioni fraudolente. Si osservi la sicurezza delle carte di credito: ecco dove si troveranno idee per una soluzione a

questo problema.

Purtroppo, finché le istituzioni finanziarie non saranno responsabili di tutte le perdite associate al furto d'identità, e non solo delle loro perdite dirette, non saremo in grado di vedere molte soluzioni. Ho già parlato anche di questo.

Le abbiamo ottenute per le carte di credito perché il Congresso ha ordinato che le banche fossero dichiarate responsabili per tutto ad eccezione dei primi 50 dollari di transazioni fraudolente.

La vicenda:

<http://www.finextra.com/fullstory.asp?id=14384>
http://www.theregister.co.uk/2005/10/12/outlaw_phishing/

Il blog di F-Secure:

<http://www.f-secure.com/weblog/archives/archive-102005.html>

Qui si parla di una vicenda analoga: la Banca della Nuova Zelanda ha sospeso l'Internet banking, preoccupata dal fenomeno del phishing. Finalmente qualcuno che sta considerando seriamente la minaccia.

<http://www.stuff.co.nz/stuff/0,2106,3450674a13,00.html>

Intanto il governo sta ordinando l'autenticazione a due fattori per le banche statunitensi:

<http://banktech.com/news/showArticle.jhtml?articleID=173401089>
<http://www.ffiec.gov/press/pr101205.htm>

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

News

Ecco un tipo di phishing che sfrutta i messaggi SMS e una telefonata.

http://www.chinadaily.com.cn/english/doc/2005-10/12/content_484196.htm

oppure <http://tinyurl.com/bvz3q>

Richiesto il passaporto per poter usare Internet in Italia. Perché? Per il terrorismo, naturalmente.

<http://www.csmonitor.com/2005/1004/p07s01-woeu.html>

Molte stampanti laser a colori racchiudono informazioni segrete in ogni pagina che stampano, sostanzialmente per potervi identificare. Qui l'EFF ha craccato il codice della serie DocuColor di stampanti Xerox.

<http://www.eff.org/Privacy/printers/docucolor/>
http://news.com.com/2300-1029_3-5901948-1.html
<http://www.washingtonpost.com/wp-dyn/content/article/2005/10/18/AR2005101801663.html>

Il Regno Unito si è servito di leggi antiterrorismo per soffocare la libertà di espressione:

http://www.schneier.com/blog/archives/2005/10/terrorism_laws.html

Ora le sta usando per tenere i pedoni fuori dalle piste ciclabili:

<http://women.timesonline.co.uk/article/0,,17909-1829289,00.html>

E per vietare alle persone di fotografare le autostrade:

http://www.dailyecho.co.uk/hampshire/southampton/news/SOTON_NEWS_NEWS0.html

Ora, io capisco che il terrorismo è la minaccia del momento, e che ogni sorta di azioni intraprese dai governi vengano giustificate con il terrorismo, ma tutto questo è ridicolo.

La polizia sta richiedendo l'accesso a webcam private:

[http://www.pe.com/localnews/corona/stories/PE News Local C cwatch05.13a cfd04.html](http://www.pe.com/localnews/corona/stories/PE%20News%20Local%20C%20watch05.13a%20cfd04.html) oppure <http://tinyurl.com/c5rrz>

Fra quanto una legge che obblighi queste webcam a essere costruite con una backdoor per la polizia?

Questo è un articolo semplicemente delizioso. Molto sottile.

http://www.theregister.co.uk/2005/04/27/security_for_the_paranoid/

Una rassegna bizzarra ed esilarante di poster governativi che richiamano alla sicurezza.

<http://www.defensetech.org/archives/001862.html>

"Uno studio rivela come Pittsburgh sia impreparata a sostenere un attacco in massa di zombie".

<http://www.theonion.com/content/node/41676>

Una vicenda assolutamente sconcertante, risalente ai primi anni Novanta, in merito a prelievi bancomat fantasma e al sistema bancario britannico (la storia è dei primi anni Novanta ed è stata appena resa pubblica). Si legga come un sistema di sicurezza assai farraginoso, unito a banche che si servono di sistemi legali per evitare di risolvere il problema, abbia portato molte vittime innocenti a perdere denaro a causa di prelievi fantasma. Si legga come siano stati tutti molto fortunati che tale catastrofico problema di sicurezza non sia mai stato scoperto dai criminali. È una vicenda incredibile.

http://www.theregister.co.uk/2005/10/21/phantoms_and_rogues/

Sui prelievi fantasma si veda anche la pagina di Ross Anderson:

<http://www.cl.cam.ac.uk/~mkb23/phantom>

Alistair Kelman mi assicura che non ha richiesto 1.750 sterline all'ora, solo 450.

Questa è una storia interessante (accaduta sei mesi fa) che riguarda un programma fedeltà di un supermercato. La Persona 1 smarrisce un orologio di valore in un supermercato. La Persona 2 lo trova e, invece di restituirlo come vuole la legge, se lo tiene. Due anni dopo, lo riporta per farlo riparare. Il riparatore controlla il numero di serie confrontandolo in un database di oggetti smarriti. La Persona 2 non ammette di aver trovato l'orologio, sostiene invece di averlo comprato in una sorta di negozio di orologi usati. La polizia controlla i registri del programma fedeltà del supermercato e scopre che la Persona 2 si trovava nel supermercato poche ore dopo che la Persona 1 aveva dichiarato lo smarrimento.

<http://www.timesonline.co.uk/article/0,,2-1459390,00.html>

Gli abusi del Patriot Act statunitense ad opera dell'FBI:

http://www.schneier.com/blog/archives/2005/10/fbi_abuses_of_t_1.html

Una delle minacce da trama cinematografica più sciocche che abbia visto di recente: terroristi che giocano a tombola nel Kentucky.

<http://www.wkyt.com/Global/story.asp?S=4019597>

Un interessante commento sulle schede di identificazione digitali.

<http://www.chi-publishing.com/?staticID=0>

Le minacce da trama cinematografica non si limitano al terrorismo. In campo medico, l'influenza dei volatili è l'attuale minaccia da trama da film. Molte persone sono convinte di avere la malattia, pur non avendola.

<http://www.nytimes.com/2005/10/25/health/psychology/25essa.html>

Una nuova tecnologia che permette di effettuare intercettazioni attraverso i muri.

<http://www.newscientist.com.nyud.net:8090/article.ns?id=dn8208>>

Lo stato del Missouri vuole tracciare gli spostamenti delle persone tramite i telefoni cellulari.

<http://www.thenewspaper.com/news/06/696.asp>>

In Australia si sta lavorando a una nuova legge antiterrorismo. Essa prevede, fra l'altro, un periodo di 14 giorni di detenzione segreta senza arresto ad opera dei servizi di sicurezza, il potere della polizia di sparare-per-uccidere "in base a sospetti" e multe e reclusione per chi rivela che un individuo è stato oggetto di investigazione. Le notizie riportate dalla stampa sono piuttosto brutte.

<http://www.theage.com.au/news/opinion/antiterrorism-laws-threaten-media-freedom/2005/10/24/1130006058337.html>> oppure

<http://tinyurl.com/brtou>

<http://www.abc.net.au/news/newsitems/200510/s1489719.htm>>

Questa bozza di legge non avrebbe dovuto essere resa pubblica a questo punto, ma il Primo Ministro dell'ACT l'ha pubblicata sul suo sito Web a dispetto della richiesta del governo federale di non farlo.

<http://chiefminister.act.gov.au/media.asp?media=692§ion=24&title=Media%20Release&id=24>> oppure <http://tinyurl.com/74tf2>>

http://www.chiefminister.act.gov.au/docs/B05PG201_v281.pdf>

Ecco una minaccia di sicurezza che scommetto non avevate mai considerato prima: criminali con cani di grossa taglia: "Il consiglio dei sovrintendenti della Contea di Contra Costa (California) ha unanimemente sostenuto il divieto ai criminali condannati di possedere cani aggressivi o dal peso superiore a 9 kg, assicurando che la proposta diventerà legge quando verrà presentata al comitato per l'approvazione il 15 novembre". Non si tratta di criminali in prigione, ma di detenuti che sono stati rilasciati dopo aver scontato la loro pena. È loro permesso di reintegrarsi nella società, ma forse lasciar loro tenere un cane di grossa taglia sarebbe un rischio troppo grande per la comunità?

<http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2005/10/26/BAGGAFE5251.DTL&hw=contra+costa+felons+dogs&sn=001&sc=1000>> oppure

<http://tinyurl.com/92fxn>>

I giudici hanno vietato alla polizia di usare i telefoni cellulari come dispositivi di tracciamento. Buone notizie, per una volta.

<http://www.wired.com/news/technology/0,1282,69390,00.html>>

Il NIST ha tenuto un laboratorio di hash crittografico per discutere di che cosa fare sulla scia dei recenti attacchi crittanalitici ai danni di SHA-1. Ricca e interessante discussione; nessuna conclusione se non quella che sono necessarie ulteriori ricerche e discussioni. Ho dato aggiornamenti dell'evento in tempo reale sul mio blog.

http://www.schneier.com/blog/archives/2005/10/nist_hash_works_1.html>

http://www.schneier.com/blog/archives/2005/10/nist_hash_works_2.html>

http://www.schneier.com/blog/archives/2005/10/nist_hash_works_3.html>

http://www.schneier.com/blog/archives/2005/11/nist_hash_works.html>

http://www.schneier.com/blog/archives/2005/11/nist_hash_works_4.html>

La faccenda dei brevetti segreti della NSA è ingiusta:

<http://www.newscientist.com/article.ns?id=dn8223>>

http://blog.wired.com/elsewhere/index.blog?entry_id=1264879>

Autenticare le persone in base ai loro pattern dattilografici:

http://pc50461.uni-regensburg.de/ibi/de/leistungen/research/projekte/ri-sk/psylock_english

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

Ho spesso parlato di come le discussioni sulla sicurezza riguardino la sicurezza molto raramente. Ecco una storia che illustra proprio questo.

A una madre nel New Jersey non piace che lo scuolabus di suo figlio si fermi da McDonald's tutti i venerdì mattina. Apparentemente incapace di trovare un'argomentazione convincente contro queste fermate (il che onestamente mi sembra strano: a me ne verrebbero in mente più d'una), si appella a minacce da trama cinematografica: "Tyler vuole che le fermate siano soppresse per paura che uno studente venga investito da qualcuno nella corsia di accesso, o che vi sia una rapina nel fast food mentre suo figlio e altri studenti si trovano all'interno".

<<http://www.nj.com/news/bridgeton/index.ssf?/base/news-0/1130146898119640.xml&coll=10>> oppure <<http://tinyurl.com/dqj8v>>

Uno studio interessante sull'algoritmo di Oracle per l'hashing delle password.

<<http://www.sans.org/info/911/>>

Questo affascinante studio di ricerca parla delle vulnerabilità del sistema di trasmissione della marina militare statunitense negli anni Ottanta. Come ricorderete, John Walker e i suoi seguaci passarono ai sovietici i segreti che avrebbero permesso di effettuare intercettazioni su questo sistema.

<<http://www.fas.org/irp/eprint/heath.pdf>>

Il MIT sta implementando un network wireless di sorveglianza 24 ore su 24, 7 giorni su 7:

<http://news.yahoo.com/s/ap/20051103/ap_on_hi_te/wireless_campus>

Il WiFi è certamente un'ottima tecnologia per questo tipo di sorveglianza su vasta scala. È una tecnologia aperta e ben standardizzata che permette a tutti di entrare nel business della sorveglianza. Bluetooth è una tecnologia analoga: aperta e facile da usare. Le tecnologie dei telefoni cellulari, invece, sono chiuse e proprietarie. RFID potrebbe essere la tecnologia di sorveglianza preferita in futuro, a seconda di quanto aperta e standard diventerà.

Credo che questo sistema di cattura dati istantanea sia un precursore di ciò che vedremo in futuro.

<<http://www.cioinsight.com/article2/0,1397,1878051,00.asp>>

Microsoft vuole una legge nazionale sulla privacy. Avete capito bene. Microsoft sta facendo un lavoro migliore sulla privacy, di recente. Di certo il diavolo sta nei dettagli, ma questo è un buon inizio.

<http://www.schneier.com/blog/archives/2005/11/microsoft_calls.html>

Un'entrata di blog davvero ottima sulle lettere di sicurezza nazionale, usate sempre più dall'FBI per raccogliere informazioni personali senza alcuna supervisione giudiziaria.

<http://talkleft.com/new_archives/013011.html>

E un eccellente articolo di cronaca:

<<http://www.washingtonpost.com/wp-dyn/content/article/2005/11/05/AR2005110501366.html>>

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

L'ACLU ha contestato aspramente la legalità delle lettere di sicurezza nazionale.

<<http://www.aclu.org/NationalSecurity/NationalSecurity.cfm?ID=19345>>

Questa è una sorpresa: Richard Clarke ha raccomandato alla città di New York di eseguire quelle inutili perquisizioni in metropolitana. Leggendo l'articolo del New York Times, pare che il suo obiettivo non era quello di impedire atti terroristici, ma semplicemente di spostare l'attenzione di potenziali terroristi altrove... Magari sulla metropolitana di Boston.

<<http://www.nytimes.com/2005/11/07/nyregion/07search.html>>

Un gruppo dell'Agenzia Federale Tedesca per la Sicurezza

dell'Information Technology ha fattorizzato un numero a 193 cifre. (Nota: non si tratta di un record; in maggio è stato fattorizzato un numero a 200 cifre. Ma vi è un premio in denaro associato a questa iniziativa).

<http://mathworld.wolfram.com/news/2005-11-08/rsa-640/>

Fare lo sniffing di password è facile e divertente:

http://www.infoworld.com/article/05/11/04/450Psecadvise_1.html

Sarei interessato ad analizzare quel database di password. Qual è la percentuale di parole inglesi usate come password? Quante si trovano nei comuni dizionari di password? Quante utilizzano un misto di lettere maiuscole e minuscole, o numeri, o segni di interpunzione? Qual è la distribuzione della frequenza di diverse lunghezze delle password? È difficile ottenere dati di password vere e proprie. Si può scrivere un interessante studio di ricerca su quei dati.

Un utilizzo militare dello spray Silly String: trovare i cavi d'innescio di allarmi, trappole o esplosivi.

<http://www.cockeyed.com/citizen/silly/silly.html>

I miei commenti a un articolo di Business Week su transazioni azionarie fraudolente in Internet:

http://www.schneier.com/blog/archives/2005/11/fraudulent_stoc.html

http://www.businessweek.com/technology/content/nov2005/tc20051103_565150.htm oppure <http://tinyurl.com/bq92y>

Un disegno di legge dell'Illinois potrebbe vietare il possesso di lettori di schede magnetiche:

<http://www.ilga.gov/legislation/billstatus.asp?DocNum=1565&GAID=8&GA=94&DocTypeID=HB&LegID=16639&SessionID=50> oppure

<http://tinyurl.com/d6j5e>

Sky Posse è un'organizzazione, non affiliata ad alcun ente ufficiale, di persone che hanno fatto voto di reazione in caso di dirottamento aereo. I membri indossano spille molto carine, che ricordano il simbolo dello sceriffo dei film Western, con lo slogan "Ready to Roll" (pronti all'azione). Piuttosto sciocco, ma probabilmente innocuo.

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

Sulla sicurezza dei cappellini di carta stagnola:

<http://people.csail.mit.edu/rahimi/helmet/>

E una confutazione:

http://zapatopi.net/blog/?post=200511112730.afdb_effectiveness

Un rapporto secondo cui la CIA negli anni Ottanta avrebbe passato ai sovietici tecnologie contenenti bug software:

<http://www.msnbc.msn.com/id/4394002>

Hans Bethe fu uno dei primi scienziati nucleari, un membro del Manhattan Project, e un attivista politico. In un recente articolo su di lui spicca questa frase: "A volte l'insistenza su una sicurezza al 100% in realtà danneggia la nostra sicurezza, mentre una decisione coraggiosa -- anche se al momento sembra comportare certi rischi -- ci offrirà maggior sicurezza sulla lunga distanza".

<http://www.physicstoday.org/vol-58/iss-10/p52.html>

Metadati in Microsoft Office:

http://www.schneier.com/blog/archives/2005/11/metadata_in_ms.html

Vi è un nuovo rapporto emesso dai Sandia National Laboratories (scritto insieme al Lawrence Berkeley National Laboratory) intitolato "Guidelines to Improve Airport Preparedness Against Chemical and Biological Terrorism" (linee guida per migliorare la preparazione degli aeroporti

contro attacchi terroristici chimici e biologici). È segreto, ma esiste una versione accessibile al pubblico.

<<http://www.sandia.gov/news-center/news-releases/2005/def-nonprolif-sec/proact-guidelines.html>>

<<http://www.sandia.gov/news-center/news-releases/2005/images/unlsand-2005-3237.pdf>>

La NSA ha un sito dedicato ai bambini. Crypto Cat, Decipher Dog e i loro amici.

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

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

Sony installa di nascosto un rootkit sui computer

Mark Russinovich ha scoperto un rootkit sul suo sistema:

<<http://www.sysinternals.com/blog/2005/10/sony-rootkits-and-digital-rights.html>>

Dopo una serie di analisi, ha scoperto che il rootkit è stato installato come parte del software DRM collegato a un CD che aveva acquistato. Il pacchetto non può essere disinstallato. Ancor peggio, si nasconde volontariamente al sistema e non appare nell'elenco processi. Così ne ha parlato nel suo blog, sollevando un gran polverone e creando una soap opera.

Molti articoli e link disponibili nei post del mio blog:

<http://www.schneier.com/blog/archives/2005/11/sony_secretly_i_1.html>

<http://www.schneier.com/blog/archives/2005/11/more_on_sonys_d.html>

Post sul blog di Russinovich:

<<http://www.sysinternals.com/blog/2005/10/sony-rootkits-and-digital-rights.html>> oppure <<http://tinyurl.com/auyjl>>

<http://www.sysinternals.com/blog/2005/11/sony-you-dont-reeeeaaaally-want-to_09.html> oppure <<http://tinyurl.com/bpr64>>

La rimozione del rootkit è dannosa per Windows:

<http://www.theregister.co.uk/2005/11/01/sony_rootkit_drm/>

Articolo di cronaca del Washington Post:

<<http://www.washingtonpost.com/wp-dyn/content/article/2005/11/02/AR2005110202362.html>>

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

Sony mente a proposito del suo rootkit: "Questo Service Pack rimuove il componente della tecnologia di occultamento che è stata recentemente discussa in una serie di articoli pubblicati in merito alla Tecnologia XCP utilizzata sui CD musicali SONY BMG con protezione anticopia. Tale componente non è malevolo e non compromette la sicurezza. Tuttavia, per attenuare le preoccupazioni degli utenti sulla possibilità che il programma generi potenziali vulnerabilità di sicurezza, è stato rilasciato questo aggiornamento che permetterà agli utenti di rimuovere il componente dai loro computer". Ma questo aggiornamento non elimina il rootkit, toglie soltanto l'occultamento della stringa "sys".

<<http://cp.sonybm.com/xcp/english/updates.html>>

I commenti di Ed Felton:

<<http://www.freedom-to-tinker.com/?p=921>>

<<http://www.freedom-to-tinker.com/?p=923>>

<<http://www.freedom-to-tinker.com/?p=924>>

Ed è possibile servirsi del rootkit per evitare lo spyware di World of

Warcraft:

<http://www.securityfocus.com/brief/34>

F-Secure sostiene, a ragione, come questo genere di cose possa mettere a serio rischio l'affidabilità di Windows:

<http://www.f-secure.com/weblog/#00000696>

Declan McCullagh ha un ottimo articolo a riguardo. Vi saranno cause legali:

http://news.com.com/Why+they+say+spyware+is+good+for+you/2010-1071_3-5934150.html oppure <http://tinyurl.com/dmwpt>

Eccone una:

<http://business.bostonherald.com/technologyNews/view.bg?articleid=111622>

oppure <http://tinyurl.com/8s6gv>

La polizia italiana si sta interessando:

http://www.computerworld.com/securitytopics/security/story/0,10801,106064,00.html?source=NLT_PM&nid=106064 oppure <http://tinyurl.com/crgfj>

Ecco un Trojan che si serve del rootkit di Sony per nascondersi:

http://www.theregister.co.uk/2005/11/10/sony_drm_trojan/

Sony ha temporaneamente fermato la produzione di CD protetti con questa tecnologia:

<http://www.securityfocus.com/brief/45>

<http://www.cnn.com/2005/SHOWBIZ/Music/11/11/sony.copyprotection.ap/index.html> oppure <http://tinyurl.com/a5gag>

Microsoft aggiornerà i propri strumenti di sicurezza per rilevare ed eliminare il rootkit. Il che è assolutamente sensato. Se Windows va in crash a causa del rootkit (e di altri software della stessa specie), la colpa ricadrà su Microsoft.

http://news.com.com/Microsoft+will+wipe+Sonys+rootkit/2100-1002_3-5949041.html oppure <http://tinyurl.com/bmw8g>

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

Revisione periodica del DMCA

L'Ufficio Copyright della U.S. Library of Congress sta conducendo la revisione periodica obbligatoria delle disposizioni anti-raggiro del Digital Millennium Copyright Act. Si possono aggiungere commenti via Internet fino al 1° dicembre.

<http://www.copyright.gov/fedreg/2005/70fr57526.html>

Il form per commentare:

http://www.copyright.gov/1201/comment_forms

Buone fonti di informazione sul DMCA:

<http://www.eff.org/IP/DMCA/>

<http://www.epic.org/privacy/drm/>

<http://www.anti-dmca.org/>

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

Le News di Counterpane

Schneier terrà il keynote alla InfoSecurity Conference di New York l'8 dicembre.

<http://www.infosecurityevent.com>

Qui si parla della mia utility per le password, Password Safe:

<http://www.washingtonpost.com/wp-dyn/content/article/2005/10/15/AR2005101500178.html>

oppure <http://tinyurl.com/a2afk>

Password Safe:

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

Counterpane ha pubblicato un'analisi delle tendenze degli attacchi che vediamo durante le operazioni di monitoring di sicurezza. Stiamo osservando qualcosa come 500 network in 35 paesi diversi, per cui è piuttosto interessante.

<http://www.counterpane.com/pr-20051115.html>

<http://www.counterpane.com/cgi-bin/attack-trends2.cgi>

** **

Taser Cam

Il produttore dei Taser, Taser International, Inc., ha commercializzato una Taser Cam. Il dispositivo viene montato sui Taser e registra l'audio e il video ogni volta che l'arma viene attivata, a prescindere dal fatto che sia utilizzata o meno.

È un'idea analoga all'avere telecamere che registrano tutti gli interrogatori della polizia, o che registrano gli interventi della polizia stradale. Aiuta a proteggere la popolazione dagli abusi della polizia, e aiuta la polizia a difendersi dalle accuse di abuso di potere.

È in casi come questo dove le telecamere tornano utili: quando attenuano uno sbilanciamento di forze. Immaginate se potessero registrare continuamente le azioni di funzionari eletti, quando agiscono in veste ufficiale, si intende.

Naturalmente, le telecamere sono utili nella stessa misura in cui lo sono i loro dati. Se registrazioni cruciali vengono "perdute", allora non c'è responsabilità. Il sistema è piuttosto improvvisato, e la registrazione deve essere trasferita su un computer mediante un cavo USB.

Entro quando le telecamere potranno semplicemente trasferire le loro registrazioni in tempo reale in qualche affidabile deposito di sicurezza?

<http://www.local6.com/news/5263731/detail.html>

<http://www.cnn.com/2005/EDUCATION/11/08/taser.cam.ap/index.html>

** **

Un "tipico" terrorista

Un titolo davvero orribile per una vicenda apparsa sul Manila Times: "Se vedete un uomo di età compresa fra 17 e 35 anni, che indossa un berretto da baseball, con uno zaino in spalla, con in mano un telefonino e che si comporta nervosamente, è probabile che sia un terrorista".

Vediamo: ogni giorno circa 4,5 milioni di persone si servono della metropolitana di New York. Ammettiamo che l'1% di esse rientri nel profilo suddetto. Ciò vuol forse dire che ogni giorno vi sono 25.000 terroristi sulla metropolitana di New York? Mi sembra quantomeno improbabile.

Il resto dell'articolo migliora, ma insomma...

<http://www.manilatimes.net/national/2005/oct/08/yehey/top_stories/20051008top4.html> oppure <<http://tinyurl.com/d9vqz>>

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

Il worm Zotob

Se mi si perdona il paragone con gli uragani, le epidemie in Internet sono come situazioni di maltempo estremo: accadono a caso, colpiscono certi segmenti della popolazione più di altri, e il livello di preparazione accumulato in precedenza determinerà l'efficienza delle proprie difese.

Zotob è stato il primo caso di grave epidemia dai tempi di MyDoom nel gennaio 2004. È accaduto rapidamente, meno di cinque giorni dopo che Microsoft pubblicò un importante comunicato di sicurezza (il suo 39esimo dell'anno). Gli effetti di Zotob si sono grandemente differenziati da organizzazione a organizzazione: alcuni network sono stati messi letteralmente in ginocchio, altri non hanno nemmeno accusato il colpo.

Il worm ha iniziato a diffondersi domenica 14 agosto. In tutta onestà non si trattava di questo gran affare, ma ha avuto molta risonanza perché ha colpito svariate fonti di notizie importanti, prima fra tutte la CNN. Se un network di news viene direttamente colpito da qualcosa, è assai probabile che ne parlerà diffusamente. Ma la mia azienda, Counterpane Internet Security, controlla più di 500 network in tutto il mondo, e a nostro parere Zotob non meritava tutta questa attenzione da parte dei media.

Entro il 17 agosto esistevano già almeno altri dieci worm che sfruttavano la stessa vulnerabilità, ed erano sia varianti di Zotob, sia worm completamente diversi. La maggior parte di essi cercava di reclutare computer per creare network di bot, ed alcune delle varianti si facevano guerra fra loro, rubandosi in continuazione il possesso di computer. Se il vostro network è stato infettato, gli effetti sono stati disastrosi.

Due settimane più tardi, il diciottenne autore di Zotob (l'originale) è stato arrestato, insieme al 21enne che lo aveva pagato per scriverlo. Pare che il finanziatore della creazione del worm non fosse un hacker, ma un criminale a caccia di profitti.

La natura dei worm è cambiata negli ultimi anni. In precedenza, i responsabili della maggioranza dei worm erano hacker in cerca di prestigio o semplicemente intenzionati a causare danni. Oggi i worm vengono sempre più scritti o commissionati da criminali. Prendendo possesso dei computer, un worm può inviare spam, lanciare attacchi denial-of-service, o ricercare numeri di carte di credito o altre informazioni personali.

Che cosa si sarebbe potuto fare in precedenza per proteggersi da Zotob e da worm come lui? "Installare la patch" è l'ovvia risposta, ma non è una

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.