

worm e i virus hanno provocato ogni sorta di danni alle reti, ma è accaduto per caso. Nel gennaio 2003, il worm SQL Slammer ha messo fuori uso 13.000 sportelli bancomat della rete Bank of America. Ma prima che ciò accadesse, non c'era un solo esperto di sicurezza in grado di capire che quei sistemi soffrivano di quella vulnerabilità. Semplicemente, non siamo in grado di comprendere le varie interazioni a un livello tale da poter prevedere quali tipologie di attacco potrebbero portare a risultati catastrofici, e le organizzazioni terroristiche si trovano nella medesima situazione, anche se hanno tentato di rivolgersi a degli esperti.

L'esempio più prossimo a questo tipo di attacco distruttivo viene dall'Australia. Nel 2000, Vitek Boden penetrò nella rete informatica di un impianto di trattamento liquami lungo la Sunshine Coast australiana. Nel giro di due mesi, ha fatto in modo di gettare centinaia di migliaia di galloni di acque luride nei fiumi e nei parchi vicini. Alcune conseguenze: torrenti inquinati, fauna marittima distrutta, e un fetore talmente insopportabile da sollevare le proteste dei residenti. Questo è l'unico caso conosciuto in cui qualcuno si è impadronito di un sistema di controllo elettronico con l'intento di provocare danni ambientali.

Malgrado la nostra predilezione nel definire ogni cosa "terrorismo", questi attacchi non lo sono. Sappiamo che cos'è il terrorismo: è qualcuno che si fa saltare per aria in un ristorante affollato, o che manda un aereo a schiantarsi contro un grattacielo. Non è certo l'infettare computer mediante virus, o il costringere i controllori di volo a instradare manualmente gli aerei, o il disattivare una rete pager per un giorno. Queste cose provocano seccature e molta irritazione, ma non terrore.

Questo è un messaggio difficile da digerire per molti, perché ultimamente a chiunque faccia danni di una certa entità viene appioppata l'etichetta di "terrorista". Ma immaginiamoci per un momento il comando di al Qaeda riunito in una qualche caverna, che sta meditando la prossima mossa della sua jihad contro gli Stati Uniti. Uno dei capi salta su ed esclama: "Ho trovato! Disattiveremo tutte le loro e-mail...". Il terrorismo vero e proprio -- ad esempio, guidare un camion imbottito di esplosivi contro una centrale nucleare -- è ancora più semplice da realizzare, e più efficace.

Vi sono moltissimi hacker in circolazione, ragazzini in special modo, a cui piace giocare alla politica e travestire le loro buffonate da minacce terroristiche. Penetrano in sistemi di qualche altro paese (in genere non in sistemi governativi) e visualizzano un messaggio politico. Spesso si sono visti episodi simili quando due nazioni si mettono a litigare: Cina contro Taiwan, India contro Pakistan, Inghilterra contro Irlanda, USA contro Cina (durante la crisi del 2001 a seguito dell'aereo spia statunitense andato a schiantarsi sul territorio cinese), USA e Israele contro altri paesi arabi. È un fenomeno analogo a quello degli hooligan che sfogano le frustrazioni nazionali contro i tifosi di un'altra squadra di calcio straniera. È una cosa indegna e meschina, e provoca seri danni, ma si tratta di cyber-teppismo, non di cyber-terrorismo.

Vi sono svariate organizzazioni che tengono traccia degli attacchi che avvengono in Internet. Negli ultimi sei mesi, meno dell'1% degli attacchi è stato causato da paesi che si trovano nella watch list del cyber-terrorismo stilata dal governo USA, mentre il 35% proviene dall'interno degli Stati Uniti. La sicurezza informatica è ancora di primaria importanza. La gente tende a ingigantire i rischi del cyber-terrorismo e a sminuire i rischi del cyber-crimine. La frode e lo spionaggio sono problemi gravi. Fortunatamente, le stesse contromisure pensate per difendersi dai cyber-terroristi ostacoleranno anche gli hacker e i criminali. Anche se le organizzazioni renderanno sicure le loro reti per le ragioni sbagliate, sarà sempre un'ottima cosa da fare.

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

Le ristampe di Crypto-Gram

Crypto-Gram è attualmente al suo sesto anno di pubblicazione. I numeri precedenti coprono tutta una serie di argomenti legati alla sicurezza e si possono trovare a questo indirizzo:

Ecco un articolo molto interessante in merito all'arresto di tre hacker russi. Non si tratta di un articolo tecnico, ma parla delle condizioni socioeconomiche e delle motivazioni di questi criminali, ed anche della competenza e dell'efficacia dell'FBI.

<<http://www.washingtonpost.com/wp-dyn/articles/A2619-2003May17.html>>

<<http://www.washingtonpost.com/wp-dyn/articles/A7774-2003May18.html>>

<<http://www.washingtonpost.com/wp-dyn/articles/A12984-2003May19.html>>

Ottenere un documento d'identità con fototessera fasullo nel New Jersey:

<http://wcbs880.com/njnews/NJ--FakeLicenses-jn/resources_news_html>

Un altro articolo sulla questione dell'applicazione o meno delle patch di sicurezza:

<<http://www.theregister.co.uk/content/55/30605.html>>

Un buon articolo su come si possa salvaguardare la privacy a dispetto del programma di "totale consapevolezza dell'informazione" (Total Information Awareness):

<<http://www.washingtonpost.com/wp-dyn/articles/A25316-2003May7.html>>

Studio sulle motivazioni degli aggressori informatici: attacchi casuali e attacchi mirati:

<http://news.com.com/2010-1071_3-1001016.html>

Le videocamere nei telefoni cellulari sono uno strumento potenziale per comprare le elezioni. Uno dei principi basilari di una buona elezione è che il voto sia a scrutinio segreto. Qualcuno può offrirsi di comprare un voto, ma il compratore non ha alcuna garanzia che il venditore si libererà della privacy della cabina elettorale. Ma le videocamere nei telefoni cellulari hanno la potenzialità di cambiare tutto questo; il compratore può richiedere, prima di pagare, la prova di un voto comprato

<<http://news.bbc.co.uk/2/hi/technology/3033551.stm>>

Attacco dall'interno alla Coca-Cola:

<<http://www.ajc.com/business/content/business/coke/0503/14breakin.html>>

Le scatole nere installate sulle automobili, originariamente pensate per stabilire la causa di morte in un incidente stradale, vengono sempre più utilizzate in tribunale. Sulla base del loro contenuto, le persone possono essere mandate in prigione o essere ritenute responsabili. Ma dato che il sistema non è stato progettato per un impiego in sede giudiziaria, suppongo che la sicurezza di questi dispositivi sia minima.

<http://story.news.yahoo.com/news?tmpl=story&u=/usatoday/20030516/ts_usatoday/5165217> oppure <<http://tinyurl.com/bwzm>>

Hacking ai danni della privacy dei clienti in DirecTV:

<<http://www.geocities.com/foogert99/>>

Un nuovo sistema biometrico: identificare le persone in base al loro modo di camminare. Il primo articolo assicura che tale sistema "abbia avuto una percentuale di successi dell'80-95% nell'identificazione delle persone". Bisogna però fare molta attenzione a questi valori, perché non vogliono dire nulla se non si hanno sufficienti informazioni in merito a come siano stati stabiliti.

<<http://www.securityfocus.com/news/4909>>

<<http://www.nandotimes.com/technology/story/892547p-6218025c.html>>

La polizia di Seattle aveva bisogno del campione di DNA di un sospettato, per cui gli ha inviato una lettera, facendo in modo che rispondesse con una lettera in busta chiusa, busta leccata da lui stesso. Hanno così avuto un campione di DNA sufficiente a collegare il sospettato al crimine commesso.

<<http://www.cnn.com/2003/LAW/05/21/old.murder.ap/index.html>>

Il programma di "totale consapevolezza dell'informazione" (Total Information Awareness) del Pentagono ha un nuovo nome: "consapevolezza dell'informazione sul terrorismo" (Terrorism

Information Awareness).

<<http://www.msnbc.com/news/916028.asp?0cv=TA00&cp1=1>>

<http://news.com.com/2100-1028_3-1008395.html>

<<http://www.wired.com/news/privacy/0,1848,58936,00.html>>

Il rapporto al Congresso in merito al programma Terrorism Information Awareness ("Report To Congress Regarding the Terrorism Information Awareness Program") della DARPA:

<http://www.darpa.mil/body/tia/tia_report_page.htm>

Il Dipartimento della Sicurezza Nazionale sta organizzando un reparto per la sicurezza informatica. Sospetto che si tratti più di una manovra politica, ma potrebbe anche dare risultati positivi.

<<http://www.washingtonpost.com/wp-dyn/articles/A56254-2003May14.html>>

<<http://www.fcw.com/fcw/articles/2003/0512/web-cyber-05-14-03.asp>>

I problemi con alcune attuali linee di condotta delle cyber-assicurazioni:

<<http://securityfocus.com/columnists/163>>

Offerta un'assicurazione contro i furti di identità:

<http://www.forbes.com/2003/05/29/cx_ds_0529simons.html>

Molte aziende stanno usando la "sicurezza" come scusa per aggirare ogni genere di disposizione governativa:

<http://online.wsj.com/article_email/0,,SB10541572621041000,00.html>

Un giornalista ha realizzato una falsa intestazione di carta da lettera e l'ha usata per ordinare la ricetta del gas nervino e una quantità sufficiente dei quattro prodotti chimici per fabbricarne abbastanza da uccidere decine di migliaia di persone. C'è ancora la piccola questione della distribuzione (che non è semplice come sembra), ma pare che per fabbricare questa roba siano sufficienti le nozioni basilari di un chimico e un'attrezzatura da laboratorio a basso costo e facilmente recuperabile.

<<http://news.bbc.co.uk/1/hi/uk/2948900.stm>>

Questa ricerca sui sistemi per ingannare la sicurezza biometrica non è nuova, ma non ricordo di aver mai visto prima una vera e propria traduzione dell'articolo principale. Esso tratta gli scanner di impronte digitali, i sistemi di riconoscimento facciale e gli scanner dell'iride.

<<http://www.heise.de/ct/english/02/11/114/>>

<<http://www.extremetech.com/article2/0,3973,13919,00.asp>>

La sicurezza delle linee aeree statunitensi è più che altro di facciata:

<<http://www.computerworld.com/securitytopics/security/story/0,10801,81428,00.html>> oppure <<http://tinyurl.com/e8gj>>

<<http://www.salon.com/news/feature/2003/06/10/missiles/index.html>>

Uno studente hacker viene processato come un adulto. A mio parere, questo è indice del livello di isteria attuale. Fare dell'hacking sul computer della scuola equivale a pasticciare con lo spray i muri dei gabinetti. Non dovrebbe essere considerato come un reato grave, e il ragazzo non dovrebbe essere sottoposto a processo come un adulto.

<<http://www.cnn.com/2003/TECH/internet/06/10/school.hacked/index.html>>

Buona serie di commenti sulla sicurezza informatica degli USA da parte dell'ex capo Richard Clarke.

<<http://www.eweek.com/category2/0,3960,1108625,00.asp>>

Il manuale "Keeping Your Jewish Institution Safe" ("come proteggere la propria istituzione ebraica") pubblicato dalla Anti-Defamation League, è a tutti gli effetti un buon manuale di

sicurezza e di antiterrorismo.
<<http://www.adl.org/security/safe.pdf>>

Sono felicissimo che la rete wireless del dipartimento di polizia dell'Idaho stia "usando un protocollo di crittografia proprietario difficile da violare".
<<http://www.computerworld.com/mobiletopics/mobile/story/0,10801,80849,00.html>> oppure <<http://tinyurl.com/e8gm>>

I cyber-criminali sono un pericolo maggiore rispetto ai cyber-terroristi. No, non l'ho detto io... ma avrei potuto benissimo.
<<http://www.computerweekly.com/articles/article.asp?liArticleID=122331>>

Esiste un prodotto chiamato CryptoGram. Non ho idea se sia un buon prodotto, ed alcune delle dichiarazioni di marketing mi hanno fatto trasalire. Ma per la cronaca, non ho niente a che spartire con questa azienda francese.
<<http://www.cryptogram-fr.com/english/>>

Decisioni di sicurezza totalmente irrazionali provocate dalla paura (vedi sopra).
<<http://www.globetechnology.com/servlet/story/RTGAM.20030605.gtwkapi/BNStory/Front/>> oppure <<http://tinyurl.com/e8gp>>

Bozza di progetto di esposizione della vulnerabilità da parte del gruppo industriale chiamato "organizzazione per la sicurezza di Internet" ("Organization for Internet Safety").
<<http://www.oisafety.org/process.html>>

Gli articoli a riguardo:
<<http://www.securityfocus.com/news/5458>>
<http://zdnet.com.com/2102-1105_2-1013423.html?tag=printthis>

Il Dipartimento della Sicurezza Nazionale degli USA ora possiede una divisione per la sicurezza informatica nazionale (National Cyber Security Division), che accorperà il Critical Infrastructure Assurance Office (CIAO), il National Infrastructure Protection Center (NIPC), il Federal Computer Incident Response Center (FedCIRC) e il National Communications System. Non è stato detto ancora nulla su chi sarà a capo di tutto questo.
<<http://www.washingtonpost.com/ac2/wp-dyn/A24147-2003Jun6>>
<http://www.gcn.com/vol1_no1/daily-updates/22360-1.html>
<<http://www.govexec.com/dailyfed/0603/060603td1.htm>>
<<http://www.securityfocus.com/news/5544>>

** **

Le news di Counterpane

Counterpane ha un nuovo vicepresidente del settore Vendite su scala Mondiale e un nuovo vicepresidente del settore Strategia e Sviluppo.
<<http://www.counterpane.com./pr-hs.html>>

Botta e risposta con Schneier sulla sicurezza pubblicato dalla rivista Washington Technology:
<http://www.washingtontechnology.com/news/17_24/last-byte/20324-1.html>

** **

Note di sicurezza da ogni dove: i taser e gli audit di sicurezza

>1) La crittografia di comunicazioni telefoniche è molto insolita. Sedici casi di crittografia su >1358 intercettazioni è poco più dell'un per cento. Quasi nessun sospettato utilizza la >crittografia vocale.

>

>2) La crittografia di comunicazioni telefoniche non è molto efficace. Ogni volta che le forze >dell'ordine hanno trovato della crittografia, non hanno avuto problemi ad aggirarla. Presumo >che i locali commissariati di polizia non abbiano, per fare un esempio, i mezzi per >decodificare chiavi DES con attacchi brute-force. Ritengo quindi che in quei casi la >crittografia vocale sia stata piuttosto facile da aggirare.

Se queste persone usassero telefoni GSM? I telefoni GSM vengono criptati utilizzando A4 (in teoria). È anche vero che per intercettare una comunicazione su un telefono GSM non è necessario forzare A4, ma è sufficiente intercettare le stazioni base.

Applicando questa osservazione al rapporto, si potrebbe dire che "vi sono stati 16 casi di intercettazione" voglia dire semplicemente che "avevano telefoni GSM, e non abbiamo dovuto preoccuparci della crittografia perché siamo andati ad ascoltare le loro conversazioni alle stazioni base o agli switch gateway fra l'operatore mobile e quello di linea fissa (o altro operatore mobile)".

Così funziona l'intercettazione di telefoni cellulari in Europa...

Questo naturalmente non vuole mettere in discussione il discorso che si stiano vendendo dei prodotti-burla per la crittografia telefonica, ma completa semplicemente il quadro della situazione e mette in evidenza la necessità di capire a che punto termina la crittografia in una conversazione...

Da: Anonimo

Oggetto: Presupposizioni eccessive in "Crittografia e intercettazioni telefoniche"

Il rapporto della corte sulla crittografia e le intercettazioni telefoniche è interessante, ma non necessariamente basato sui fatti. Come lei stesso ha notato, è improbabile che i vari dipartimenti di polizia locali possano svolgere attacchi di forza bruta contro chiavi DES. Partendo dal fatto che alcune conversazioni erano criptate ma nessuna di esse "ha impedito ai funzionari delle forze dell'ordine di ottenere il testo in chiaro delle comunicazioni intercettate", lei ha presupposto che i funzionari sono stati in grado di decodificare i sistemi di crittografia.

Altre possibili spiegazioni potrebbero essere:

- I rapporti sulla crittografia sono sbagliati. Questo potrebbe essere dovuto alla non esatta comprensione del termine "criptato" da parte degli ufficiali incaricati del rapporto, oppure perché costoro hanno deciso di mentire intenzionalmente in modo da fare bella figura.

- I rapporti che affermano che la crittografia non avrebbe impedito alle forze dell'ordine di ottenere il testo in chiaro sono sbagliati. Non è difficile credere che un agente di polizia mentirebbe a questo proposito, soprattutto se qualcuno è stato arrestato in base ad accuse inventate ma si è voluto far credere che esistevano delle prove.

Per me entrambe queste spiegazioni sono molto più plausibili del ritenere che dipartimenti di polizia locali (o anche i federali) siano sufficientemente in gamba da aggirare un sistema di crittografia.

Da: "Israel, Howard M (Howard)" <hisrael@avaya.com>
Oggetto: Crittografia e intercettazioni telefoniche

Credo che lei abbia fatto alcune assunzioni che si rivelano essenziali per le conclusioni a cui giunge. In breve, il testo riportato non indica specificatamente che la crittografia sia stata effettivamente aggirata dalle forze dell'ordine. Forse che: 1) le forze dell'ordine abbiano minacciato di intentare un processo (presentando un mandato) contro i fornitori della tecnologia per ottenere le chiavi?; 2) le forze dell'ordine avevano molteplici sistemi per intercettare comunque una conversazione (ad esempio, la conversazione telefonica criptata ha avuto luogo in un'auto e la voce criptata era al telefono, ma nell'auto era stata piazzata anche una cimice)? 3) Forse il testo in chiaro è stato ottenuto da un dispositivo di registrazione di un informatore che era presente durante la conversazione? 4) Forse la conversazione criptata non era in effetti pertinente al caso, e quindi non necessaria alle accuse?

Queste sono soltanto alcune ipotesi. Pertanto, credo che le sue conclusioni riguardo all'apertura non siano giustificate.

Da: Mike Schiraldi <mgs21@columbia.edu>
Oggetto: Indirizzi e-mail specifici e spam

Quando utilizzavo i servizi di 1-800-Flowers avevo attivato un account del tipo flowers@eccetera, e dopo circa un anno ho improvvisamente cominciato a ricevere una miriade di spam pornografico a questo indirizzo. L'addetto del servizio clienti mi ha assicurato che la loro compagnia non condivide con nessun altro gli elenchi degli indirizzi e-mail, e gli credo. Sono sicuro che un amministratore di database, o anche un impiegato temporaneo, abbia svolto una rapida query SQL e abbia salvato i risultati su un disco, per poi venderli agli spammer. Perciò, anche se ci si fida del generale comportamento di un'azienda, occorrerebbe sempre tener presente che qualsiasi indirizzo e-mail fornito loro possa diventare di pubblico dominio con facilità.

Da: "Aram Compeau" <aram@tibco.com>
Oggetto: Indirizzi e-mail specifici e spam

Non è questa una cosa analoga allo scegliere password difficili da indovinare? Uno schema leggermente migliore può essere quello di usare <nome opzionale>_counterpane_<data e ora della sottoscrizione>@xyz.dominio. Può essere utile per ovviare al problema di fornire un altro indirizzo e-mail nel caso si voglia ritirare <counterpane@foo.com>, ma si intenda sempre fare la sottoscrizione. Con il nuovo schema è possibile ritirare <counterpane_051520031044@foo.com> e generare <counterpane_051620031030@foo.com>. Naturalmente possono esserci infinite varianti del suffisso. Finché si utilizza un sistema del genere, in caso di errore e/o dolo accidentale sarà difficile essere incastrati.

Da: "Brent J. Nordquist" <brent@nordist.net>
Oggetto: Contromisure per prevenire i furti dei dipendenti

Lei ha scritto:

>Una pratica di sicurezza molto usata è quella di mettere un cartello sulla cassa, che dice: "Il vostro acquisto è gratuito se mi dimentico di darvi lo scontrino". Con questo cartello il cliente è invitato a notare se gli venga dato o meno lo scontrino e a "segnalare" l'addetto da cui non l'ha ricevuto (pretendendo che l'acquisto sia considerato gratuito). Questo rende il cliente una sorta di agente di sicurezza contro i furti degli impiegati: è in grado di far fronte a questa "funzione di sicurezza" e l'incentivo è dato dal cartello.

Un simile scenario di cui sono stato testimone è il rischio che l'addetto dica al cliente "Fanno \$7,73" mentre in realtà sono solo \$6,73, e intanto si intaschi il dollaro in più. Di conseguenza mi è capitato di vedere (agli autogrill Taco Bell e in altri posti) un grosso display a LED luminoso indicante il prezzo, e un avviso collocato poco più sotto che dice "Chiamare il 1-800-XXX-XXXX se vi viene chiesto di pagare un importo diverso da quello mostrato".

Da: Robert Hannent

Oggetto: Sicurezza nei campi da gioco

Mentre studiavo all'università, mi serviva del denaro extra per pagarmi le spese, e allora per disperazione ho iniziato a lavorare nell'ambito della sicurezza degli stadi di calcio. Ho persino fatto un corso di addestramento ufficiale con la Football Stewards Association. Il problema delle bottiglie era davvero grave nel calcio inglese e negli eventi sportivi che si svolgono su di un campo. L'attacco tipico consisteva nel portare all'interno dello stadio una bottiglietta di qualche bevanda gassata, e una volta svuotata, riempirla di nuovo con urina o altri fluidi corporei. Poi la si tirava contro un giocatore fermo o verso i tifosi dell'altra squadra. Se la vittima era fortunata, veniva solo colpita su una parte del corpo; lo sfortunato, invece, se la beccava in testa e la bottiglia, rompendosi, liberava il suo contenuto.

Le lattine non sono mai state una minaccia vera e propria, anche se negli stadi inglesi vi sono stati problemi legati all'alcool a cui si è posto rimedio. La problematica principale legata alle lattine potrebbe riguardare la costruzione di un'arma affilata partendo dalla lattina di alluminio.

Come ha affermato il signor Belloc, non importa se si affronta il problema di armi propulsive di grosse dimensioni; gli strumenti più piccoli sono sempre a disposizione. Per molto tempo un grave problema nello sport inglese era dato dall'uso di certe monete -- soprattutto la moneta inglese da 50 pence, che non è rotonda, ma sfaccettata, e in precedenza era anche più pesante. Tuttavia, di recente, con l'introduzione della pesante moneta da due sterline, molti criminali hanno trovato il suo peso e la sua aerodinamica davvero utili.

Un aspetto della violenza da stadio, che ho trovato molto illuminante durante la mia esperienza, è stata la scoperta che molta della violenza all'interno dei gruppi di supporter è coordinata. Vi sono gruppi di fanatici che amano la violenza e stabiliscono un'ora e un luogo per incontrarsi a fare "mischia". Io ho lavorato presso uno stadio modernamente attrezzato, con pochi incidenti causati da violenza all'interno della struttura, grazie anche ad un esperto controllo della folla e da un sistema di circuito chiuso flessibile ad ampio raggio.

Il problema più grosso è quel che accade fuori dallo stadio, e questa moderna struttura si serve della propria tecnologia per aiutare le forze dell'ordine segnalando con telefoni cellulari gli individui che vengono visti organizzare gli atti di violenza. La collaborazione coordinata fra la sicurezza e le forze dell'ordine è estremamente importante per mantenere un certo livello di protezione.

Da: "Robert P. Goldman" <rpgoldman@sift.info>

Oggetto: Sicurezza nei campi da gioco

Tutte le e-mail in merito a questo argomento mi hanno fatto venire in mente qualcosa che non posso fare a meno di segnalare: la stessa restrizione di sicurezza viene impiegata a New Orleans, tranne che nelle strade. È possibile bere bevande alcoliche in pubblico, ma devono essere in tazze di plastica, in modo che nessuno possa farsi male...

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

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

La versione italiana è curata da Communication Valley SpA
<http://www.communicationvalley.it/>.

Per iscriversi o cancellarsi andare all'indirizzo <http://www.cryptogram.it/>.

I numeri arretrati sono disponibili all'indirizzo <http://www.cryptogram.it/>.
Per informazioni crypto-gram@communicationvalley.it.

Inoltrate liberamente CRYPTO-GRAM a colleghi ed amici che possano trovare la rivista interessante. Viene concessa l'autorizzazione a ristampare CRYPTO-GRAM, a condizione che sia stampata integralmente.

CRYPTO-GRAM è realizzata da Bruce Schneier. Schneier è il fondatore e CTO di Counterpane Internet Security, Inc., autore di "Secrets and Lies" e di "Applied Cryptography" e inventore degli algoritmi Blowfish, Twofish e Yarrow. È membro del comitato consultivo dell'Electronic Privacy Information Center (EPIC). Scrive spesso e tiene conferenze in merito alla sicurezza informatica e alla crittografia.

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) 2003 by Counterpane Internet Security, Inc.