

CRYPTO-GRAM
15 agosto 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:

Profiling

Cisco e ISS minacciano un ricercatore di sicurezza

Revoca di una deliberazione sull'intercettazione di email

Rubare merce immaginaria

Le ristampe di Crypto-Gram

Disattivare i telefoni cellulari nelle gallerie

Perquisizione delle borse nelle metropolitane

Plagio e mondo accademico: un'esperienza personale

Rivista la sicurezza dei passaporti RFID

I rischi legati alla perdita di dispositivi portatili

Come non risolvere il problema dei documenti d'identità

Secure Flight

News

Sparare per uccidere

Le News di Counterpane

Visa e American Express abbandonano CardSystems

Commenti dei lettori

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

Profiling

Da quando è avvenuto l'attentato terroristico a Londra, si è parlato molto a proposito del profiling. Ecco quel che ho scritto sull'argomento in "Beyond Fear" (pagg. 133-137):

"Una buona sicurezza è affidata alle persone. Le persone sono versatili, possono improvvisare, essere creative, possono sviluppare soluzioni al momento, possono rilevare aggressori mentre imbrogliano e tentare di mantenere la sicurezza malgrado l'imbroglio. Le persone possono rilevare malfunzionamenti o guasti passivi e cercare di porvi rimedio. Le persone sono

l'elemento più forte in un procedimento di sicurezza. Quando un sistema di sicurezza ha successo contro un attacco nuovo o coordinato o devastante, solitamente è dovuto agli sforzi delle persone.

"Il 14 dicembre 1999, Ahmed Ressam tentò di penetrare negli Stati Uniti su un traghetto partito da Victoria Island, British Columbia. Aveva una valigetta esplosiva nel baule della sua automobile. Il suo piano era guidare fino al Los Angeles International Airport, mettere la valigetta su un carrello all'interno del terminal, impostare il timer e andarsene. Il piano avrebbe funzionato se qualcuno non fosse stato all'erta.

"Ressam doveva passare la dogana prima di imbarcarsi sul traghetto. Aveva un documento d'identità fasullo, a nome di Benni Antoine Noris, e il computer gli ha dato l'autorizzazione basandosi su tale identità. Gli è inoltre stato consentito di passare dopo un controllo sommario del baule della sua auto, sebbene fosse ricercato dalla polizia canadese. Dall'altra parte dello Stretto di Juan de Fuca, a Port Angeles, Washington, Ressam è stato avvicinato dall'agente di frontiera USA Diana Dean, che gli ha rivolto alcune domande di routine e ha poi stabilito che l'individuo appariva sospetto. Era agitato, sudato, e nervoso. Evitava lo sguardo del suo interlocutore. Usando le parole di Dean, "aveva un'aria strana". Più aumentavano le domande (non vi era nessun altro ad attraversare la frontiera, per cui altri due agenti si sono aggiunti all'interrogatorio) e il comportamento di Ressam si faceva sempre più sospetto. L'auto di Ressam è stata poi perquisita, e lui infine scoperto e arrestato. Non è stato un dettaglio particolare a insospettire Dean, ma tutto ciò che racchiude la frase "aveva un'aria strana". Ed ha funzionato. Se non è stata piazzata una bomba nel Los Angeles International Airport intorno al Natale 1999, è grazie all'intuito e all'attenzione di un ufficiale di sicurezza addestrato e preparato.

"C'è una 'parolaccia' che descrive ciò che ha fatto Dean quel freddo pomeriggio di dicembre: profiling. Tutti lo praticano in qualsiasi occasione. Quando vedete qualcuno nascondersi in un vicolo buio e cambiate direzione per evitarlo, state effettuando un profiling. Quando il proprietario di un negozio nota qualcuno guardarsi intorno furtivamente e intanto muove le mani all'interno della propria giacca, egli sta effettuando un profiling. Le persone tracciano un profilo basandosi su come qualcuno si veste, sui suoi modi, sul suo tono di voce... e sì, anche sulla sua razza ed etnia. Quando per strada vedete qualcuno correre verso di voi brandendo un'ascia insanguinata, non siete sicuri che si tratti effettivamente di un pazzo sanguinario. Magari è un macellaio che sta rincorrendo la signora di fianco a voi per darle il resto che si è dimenticata. Ma in un modo o nell'altro farete un'ipotesi. Quell'ipotesi è un esempio di profiling.

"Tracciare un profilo significa generalizzare. Significa prendere le caratteristiche di una popolazione e applicarle a un individuo. Le persone sono portate a sviluppare un'intuizione nei confronti di altre persone basata su svariate caratteristiche. A volte tale intuizione è corretta, altre volte no, ma si tratta sempre della prima reazione di una persona. La bontà di tale intuizione come contromisura dipende da due fattori: la sua accuratezza e la sua efficacia quando viene istituzionalizzata o quando le caratteristiche del profilo diventano luogo comune.

"Uno dei modi in cui il profiling diviene istituzionalizzato è attraverso la computerizzazione. Invece di avere una Diana Dean che controlla un individuo, un calcolatore controlla il profilo e ne dà una certa valutazione. In genere, quei profili con valutazioni particolarmente alte vengono poi esaminati più accuratamente da persone, anche se a volte si attivano contromisure basandosi esclusivamente sul profiling elettronico. Questo è, ovviamente, più farraginoso. Il calcolatore può tracciare profili basandosi soltanto su caratteristiche semplici e facili da assegnare: età, razza, cronologia dei crediti, storia professionale, eccetera. I calcolatori non hanno la sensazione che qualcuno possa "avere un'aria strana", né possono adattarsi a una situazione come fanno le persone.

"Il profiling funziona meglio se le caratteristiche del profilo sono precise. Se una guida irregolare è un buon indizio dello stato di ebbrezza del conducente, allora per un agente di polizia questa sarà una buona caratteristica in base alla quale decidere chi fermare. Se il guardarsi intorno

furtivamente in un negozio o l'indossare un cappotto in una giornata calda sono buoni indicatori per stabilire che una persona è un taccheggiatore, allora saranno anche buone caratteristiche a cui il proprietario del negozio dovrà prestare attenzione. Ma se l'indossare pantaloni flosci o oversize non è un buon indizio per stabilire che la persona è un taccheggiatore, allora il proprietario del negozio perderà un sacco di tempo tenendo inutilmente d'occhio persone oneste che hanno gusti discutibili nel vestire.

"Nel gergo comune, il termine 'profiling' non si riferisce a queste caratteristiche. Invece, fa riferimento al profiling basato su caratteristiche quali razza ed etnia, e al profiling istituzionalizzato basato unicamente su tali caratteristiche. Durante la Seconda Guerra Mondiale, gli Stati Uniti hanno radunato più di 100.000 persone di origine giapponese che vivevano sulla costa occidentale e le hanno rinchiusi in accampamenti (ovvero prigionieri). Questo è stato un esempio di profiling. Le guardie al confine israeliano passano molto più tempo a esaminare uomini arabi che non donne israeliane: un altro esempio di profiling. In molte comunità statunitensi la polizia ha spesso fermato e interrogato persone di colore che guidavano in quartieri ricchi abitati da bianchi (ci si riferisce comunemente a questo fenomeno con la sigla DWB, Driving While Black, ovvero, praticamente "guida in stato di nerezza"). In tutti questi casi si potrebbe accampare la scusa della sicurezza, ma i compromessi sono enormi: persone oneste che rientrano nel profilo possono venire disturbate, molestate o addirittura arrestate se si presume che siano aggressori.

"Per i governi democratici si tratta di un problema molto grave. È semplicemente sbagliato ridurre le persone a due categorie, 'ad alta probabilità di essere aggressori' e 'a bassa probabilità di essere aggressori' basandosi sulla razza o sull'etnia. È sbagliato che la polizia fermi un'auto solo perché i suoi occupanti di colore stavano circolando in un quartiere ricco di bianchi. Si tratta di discriminazione bella e buona.

"Ma la gente, quando ha paura, soggiace a pessimi compromessi di sicurezza, ed è per questo che abbiamo visto campi di internamento di giapponesi durante la Seconda Guerra Mondiale, e perché oggi c'è così tanta discriminazione nei confronti degli arabi negli Stati Uniti. Questo non risolve nulla, e non crea nessuna sicurezza efficace. Per quanto riguarda l'internamento dei giapponesi, per esempio, una commissione ha scritto nel 1983 che le cause dell'incarcerazione erano radicate in 'pregiudizi razziali, isteria bellica, e mancanza di leadership politica'. Ma solo perché qualcosa è sbagliato non significa che la gente smetterà di farlo.

"A prescindere da un discorso etico, il profiling istituzionalizzato non funziona perché i veri aggressori sono molto rari: gli errori attivi saranno più frequenti di quelli passivi. La stragrande maggioranza di persone che rientrano nel profilo saranno innocenti. Allo stesso tempo, alcuni veri aggressori cercheranno di sottrarsi al profilo. Durante la Seconda Guerra Mondiale, un sabotatore giapponese in America poteva cercare di evitare la prigionia fingendo di essere cinese. Analogamente, un terrorista arabo potrebbe tingersi i capelli di biondo, imparare l'accento americano, e così via.

"Il profiling può anche distogliere l'attenzione dalle minacce al di fuori del profilo. Se gli ufficiali di frontiera degli Stati Uniti fermano e perquisiscono chiunque sia giovane, maschio e arabo, non avranno tempo di fermare e perquisire ogni altro genere di individuo, non importa se questi abbia o meno un'aria strana. D'altro canto, se gli aggressori provengono tutti da una stessa razza o etnia, il profiling ha maggiori probabilità di funzionare (anche se sul piano etico la questione rimane aperta). In un'ottica di sicurezza, per la compagnia aerea El Al ha sicuramente più senso investigare giovani maschi arabi che non famiglie israeliane. In Vietnam i soldati americani non sapevano mai chi dei civili del luogo fosse in realtà un combattente; a volte la soluzione di sicurezza scelta era semplicemente ucciderli tutti.

"Se molto in questa discussione è odioso (come forse dovrebbe essere), sono i compromessi nella vostra testa che stanno parlando. È perfettamente sensato decidere di non implementare una contromisura non perché non funziona, ma perché i compromessi sono davvero eccessivi. Rinchiudere ogni persona dall'aspetto arabo ridurrà il potenziale di un terrorismo di matrice

musulmana, ma nessuna persona razionale suggerirebbe un metodo del genere (è un classico esempio del 'vincere la battaglia ma perdere la guerra'). Negli Stati Uniti vi sono leggi che vietano alla polizia di effettuare un profiling basato su caratteristiche come l'etnia, poiché crediamo che tali misure di sicurezza siano sbagliate (e non semplicemente perché le riteniamo inefficaci).

"Tuttavia, non importa quanto un governo lo renda illegale, il profiling esiste sempre a vari livelli. A livello individuale, a livello di una Diana Dean, che decide quali auto far passare e quali fermare e investigare più a fondo. Ha effettuato un profiling su Ressam basandosi sui suoi modi e sulle risposte alle domande che lei gli ha rivolto. Era algerino, particolare che lei ha certamente notato. Ma ciò accadeva prima dell'11 settembre, e i rapporti dell'incidente indicano chiaramente che Dean lo ritenesse un contrabbandiere di droga; probabilmente in questo caso l'etnia non era un fattore chiave nel profiling. Ed è questo uno degli aspetti più interessanti della storia. Quell'intuizione, quel sentire che qualcosa non quadrava ha funzionato egregiamente, anche se tutti avevano fatto un'assunzione sbagliata su ciò che era storto. L'intuizione umana ha rilevato un tipo di attacco completamente inaspettato. Gli esseri umani, in quanto a percezioni di comportamenti sospetti batteranno i computer ancora per molto tempo.

"E se fatto in maniera corretta, questo genere di profiling basato sull'intuizione può essere una contromisura di sicurezza eccellente. Dean era addestrata e aveva l'esperienza necessaria per effettuare un profiling in modo accurato e appropriato, senza esagerare sconfinando in un profiling illegale. Tutto sta nell'assicurarsi che la percezione di un rischio coincida con i rischi effettivi. Se chi è responsabile della sicurezza effettua un profiling incentrato su superstizioni e intuizioni dettate da pregiudizi, oppure seguendo alla cieca un sistema di profiling elettronico, il profiling non funzionerà affatto. Ancora peggio, può in effetti ridurre la sicurezza distogliendo le persone dalle reali minacce. Il profiling istituzionalizzato può ossificare la mente, e la mente di una persona è la misura di sicurezza più importante che abbiamo".

Altri spunti (non derivati dal mio libro):

1. Tutte le volte che si progetta un sistema di sicurezza che prevede due strade per attraversarlo, una facile e l'altra difficile, si invita l'aggressore a prendere la strada più facile. Un profiling che prende di mira giovani arabi maschi produrrà terroristi che sono vecchi, non arabi, di sesso femminile.

2. Se vogliamo aumentare la sicurezza antiterrorismo, i giovani arabi maschi che vivono negli Stati Uniti sono esattamente le persone che dobbiamo avere dalla nostra parte. Discriminarli in nome della sicurezza non li renderà di certo più inclini a collaborare.

3. Malgrado ciò che pensano in molti, il terrorismo non si limita a giovani arabi di sesso maschile. Richard Reid (quello dell'ordigno nascosto nella scarpa) era inglese. Germaine Lindsay, uno dei terroristi responsabili dell'attentato dinamitardo a Londra il 7 luglio, era afro-caribico. Di seguito vi sono altri esempi tratti da un discorso del Segretario dei Trasporti USA Norman Mineta:

"Nel 1986 una donna irlandese di 32 anni, al tempo in attesa di un figlio, stava imbarcandosi su un volo El Al da Londra diretto a Tel Aviv, quando gli agenti di sicurezza della El Al scoprirono un ordigno esplosivo nascosto nel doppio fondo della sua borsa. Era stato il fidanzato della donna (il padre del bambino che lei portava in grembo) a nascondere la bomba.

"Nel 1987, un uomo di 70 anni e una 25enne, nessuno dei due era mediorientale, hanno finto di essere padre e figlia e hanno portato una bomba a bordo di un volo Korean Air da Baghdad diretto in Thailandia. Verso Bangkok l'ordigno è esploso uccidendo tutti gli occupanti dell'aereo.

"Nel 1999 alcuni individui vestiti da uomini d'affari (e uno vestito da prete cattolico) si sono rivelati essere dei dirottatori, che hanno obbligato un volo Avianca a deviare verso una pista di

atterraggio in Colombia, dove alcuni passeggeri sono stati tenuti in ostaggio per più di un anno e mezzo”.

I terroristi dell'attentato di Bali nel 2002 erano indonesiani. I terroristi ceceni che hanno abbattuto gli aerei russi erano donne. Timothy McVeigh e Unabomber erano americani. I terroristi baschi sono baschi, e i terroristi irlandesi sono irlandesi. I Tamil Tigers sono di Sri Lanka.

E molti musulmani non sono arabi. Anzi, la maggior parte degli arabi non sono terroristi: molte persone che sembrano di origine araba non sono nemmeno musulmane. Per cui non soltanto siamo di fronte a un gran numero di falsi negativi (terroristi che non corrispondono al profilo), ma vi è anche un gran numero di falsi positivi: innocenti che corrispondono al profilo.

Beyond Fear:

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

Il discorso del Segretario dei Trasporti USA Norman Mineta:

<<http://www.dot.gov/affairs/042002sp.htm>>

Una ricerca sull'efficacia del profiling di contro a perquisizioni casuali come misura di sicurezza:

<http://www.firstmonday.org/issues/issue7_10/chakrabarti>

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

Cisco e ISS minacciano un ricercatore di sicurezza

Ho scritto più volte in merito all'esposizione totale, e su come la divulgazione di vulnerabilità di sicurezza sia il sistema migliore per migliorare la sicurezza, specialmente in un contesto di libero mercato (vale la pena di rileggere quell'articolo anche per la trattazione generale dei compromessi di sicurezza). Ho anche scritto di come le aziende legate alla sicurezza trattino le vulnerabilità prima come problemi di pubbliche relazioni e poi come problemi strettamente tecnici. Questa settimana alla conferenza BlackHat, il ricercatore di sicurezza Michael Lynn e Cisco hanno dimostrato entrambi gli argomenti.

Lynn stava per presentare alcune falle di sicurezza negli IOS di Cisco, e Cisco ha fatto l'impossibile per garantire che tali informazioni non giungessero ai propri clienti, alla stampa, all'opinione pubblica. Secondo il Wall Street Journal:

"Cisco ha minacciato azioni legali per evitare che gli organizzatori della conferenza permettessero a un 24enne ricercatore di un'azienda rivale di discutere come, a suo avviso, degli hacker possano ottenere il controllo dei router Cisco, che di fatto dominano il mercato. Cisco ha anche dato istruzioni agli impiegati di strappare dal programma della conferenza le 20 pagine che delineavano tale presentazione e ha ordinato la distruzione dei 2.000 CD che la contenevano.

"Alla fine, il ricercatore Michael Lynn ha tenuto ugualmente la presentazione, descrivendo le vulnerabilità del software Cisco che, a suo parere, potrebbero permettere agli hacker di controllare reti aziendali e governative, e Internet, intercettando e deviando le comunicazioni di dati. Lynn, indossando un berretto bianco con la scritta "Good" (Buono), ha parlato dopo essersi licenziato da Internet Security Systems, Inc. lo scorso mercoledì. Lynn ha dichiarato di essersi dimesso perché la dirigenza di ISS aveva insistito affinché egli cancellasse alcune parti fondamentali della sua presentazione".

L'intera vicenda è ancora più bizzarra di così. Inizialmente, Cisco e ISS erano favorevoli alla presentazione di Lynn dei risultati della propria ricerca. Hanno cambiato idea all'ultimo

momento. Lynn ha concesso un'intervista a Wired in cui parla di alcuni dettagli; sono impressionato dalla sua integrità in questa vicenda.

Non potendo censurare tali informazioni, Cisco ha deciso di comportarsi come se non fosse un affare di grande importanza. Da un articolo di SearchSecurity:

"In un comunicato apparso poco dopo la presentazione, Cisco ha dichiarato: "È importante notare che quanto presentato da Lynn non si tratta di una nuova vulnerabilità o difetto del software IOS di Cisco. La ricerca di Lynn esamina metodi possibili per espandere exploit di vulnerabilità di sicurezza conosciute che impattano i router". E ha continuato dichiarando che "Cisco ritiene che le informazioni presentate da Lynn alla conferenza BlackHat oggi contenevano dati proprietari ottenuti illegalmente". La dichiarazione si riferisce anche al fatto che Lynn ha detto nella sua presentazione di aver utilizzato un diffuso scompattatore di file per decomprimere l'immagine Cisco prima di effettuarne un reverse engineering e scovare la falla, il che va contro l'accordo d'uso di Cisco".

Di certo la macchina propagandistica di Cisco ha fatto gli straordinari quella settimana.

Cisco e ISS hanno anche denunciato Lynn e BlackHat. La causa è stata fissata per il giorno successivo, e vale la pena leggere i post del blog di Jennifer Granick che parlano delle trattative. L'accordo ha proibito a Lynn o a BlackHat di parlare di questa vicenda o distribuire materiali della presentazione o registrazioni della presentazione. Non che abbia avuto importanza: copie delle slide della presentazione (la versione con il nome ISS, prima che ISS cambiasse idea e si opponesse alla divulgazione) sono dappertutto su Internet.

Le implicazioni di sicurezza di tutto questo sono enormi e gravi. Se le aziende hanno il potere di censurare informazioni sui propri prodotti a loro sgradite, allora noi in quanto consumatori abbiamo meno informazioni con le quali poter fare scelte d'acquisto intelligenti. Se le aziende hanno il potere di sopprimere informazioni sulle vulnerabilità dei loro prodotti, allora non hanno alcun incentivo per migliorare la sicurezza (ho scritto a questo proposito in relazione alle chiavi e alle serrature). Se la libertà di parola è subordinata agli ordini dell'industria, allora siamo tutti molto meno sicuri.

L'esposizione totale è un bene per la società. Ma siccome aiuta anche i "cattivi" e non solo i "buoni" (si veda il mio articolo su segretezza e sicurezza per un'ulteriore discussione sui bilanciamenti), molti di noi hanno sostenuto delle linee guida per una "divulgazione responsabile" che danno ai rivenditori un vantaggio iniziale nel sistemare le vulnerabilità prima che vengano annunciate.

Il problema è che non tutti i ricercatori seguono queste linee guida. E leggi che limitano la libertà di parola apportano più danni che benefici alla società (e in ogni caso non sarebbero una soluzione definitiva al problema: non è possibile far approvare leggi simili in ogni possibile paese del mondo dove vivono i vari ricercatori di sicurezza). Pertanto l'unico modo di procedere ragionevole per un'azienda è quello di lavorare insieme ai ricercatori che la mettono in guardia da eventuali vulnerabilità, ma anche di presumere che a volte le informazioni sulle vulnerabilità potranno essere rilasciate senza preavviso.

Non riesco a immaginare le discussioni all'interno di Cisco che abbiano portato l'azienda a comportarsi come delinquenti. Non riesco a capire perché abbia deciso di attaccare Michael Lynn, BlackHat e ISS invece di trasformare la situazione in un successo di pubbliche relazioni. Non riesco a credere che pensassero davvero di poter censurare le informazioni con le loro azioni, né che la ritenessero una buona idea.

I clienti di Cisco vogliono delle informazioni. Non si aspettano la perfezione, ma desiderano conoscere la gravità dei problemi e che cosa sta facendo Cisco per risolverli. L'ultima cosa che vogliono scoprire è che Cisco cerca di soffocare la verità. Quanto segue è tratto da un articolo di Computerworld:

“Joseph Klein, senior security analyst alla divisione sistemi elettronici aerospaziali di Honeywell Technology Solutions, ha detto di aver contribuito a organizzare un incontro fra professionisti IT del governo e Lynn dopo la presentazione. Klein ha detto di essere su tutte le furie perché Cisco non ha voluto divulgare la vulnerabilità al buffer overflow nei router privi di patch. ‘Vedo già una bella causa contro Cisco venir fuori da questa vicenda’, ha dichiarato Klein”.

Neanche ISS è uscita bene da questa storia. Da un articolo di Wired:

“Alcuni anni fa correva voce che ISS tacesse determinate cose perché il suo mestiere è quello di offrire soluzioni’, ha detto [Ali-Reza] Anghaie, [un senior security engineer titolare di un’azienda aerospaziale, che era fra il pubblico alla conferenza], ‘ma ora avete avuto piena e pubblica conferma che si sottometteranno ai voleri della Cisco o della Microsoft di turno, e questo non è corretto nei confronti dei loro clienti... Se sono disposti a tirarsi indietro e piantare in asso un loro dipendente, beh, che cosa faranno per i clienti?’”.

Malgrado il loro comportamento da delinquenti, per Cisco e ISS questo si è trattato di un totale disastro a livello di pubbliche relazioni. Ora non importa ciò che diranno, noi non crederemo a una parola. Sappiamo che a trattare le loro vulnerabilità di sicurezza è il loro dipartimento per le pubbliche relazioni e non quello tecnico-ingegneristico. Sappiamo che credono che sopprimere informazioni e mettere la museruola ai ricercatori è per loro più importante che informare il pubblico. Avrebbero potuto dimostrare di mettere i propri clienti davanti a tutto, invece hanno solo mostrato come i miopi interessi industriali abbiano più importanza che non essere un’entità aziendale responsabile.

E queste sono le persone che costruiscono l’hardware che fa funzionare gran parte della nostra infrastruttura? In un certo senso, non mi sento più tanto sicuro.

Nelle settimane successive all’evento, mi è sembrato che ISS stesse perseguendo tutto questo per cattiveria. Nel caso di Cisco ritengo sia stata pura stupidità, ma penso che sia proprio cattiveria per quanto concerne ISS.

Naturalmente, gli hacker stanno lavorando alacremente per ricostruire l’attacco di Lynn e scrivere un exploit. Ciò ovviamente significa che corriamo un rischio ancor più grave rispetto a quanto accadrebbe se vi fosse soltanto un worm a sfruttare questa vulnerabilità.

La cosa triste è che avremmo potuto evitare tutto questo. Se Cisco e ISS avessero semplicemente permesso a Lynn di presentare il proprio lavoro, sarebbe stata l’ennesima oscura presentazione nel mare di oscure presentazioni che è BlackHat. Cercando di zittire Lynn, le due aziende hanno garantito due cose: 1) che la vulnerabilità è stata la storia di maggior rilievo della conferenza; 2) che qualche gruppo di hacker trasformerà la vulnerabilità in codice exploit solo per vendicarsi.

Articoli sulla vicenda:

<http://online.wsj.com/public/article/0,,SB112251394301198260-2zqDRmLtWgPF5vKgFn1qYJBjaG0_20050827,00.html?mod=blogs>

oppure <<http://tinyurl.com/82y9e>>

<http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1111389,00.html?track=NL-358&ad=523843> oppure <<http://tinyurl.com/74w8f>>

<<http://www.computerworld.com/securitytopics/security/story/0,10801,103539,00.html>>

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

<<http://www.wired.com/news/privacy/0,1848,68328,00.html>>

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

<<http://news.zdnet.co.uk/internet/security/0,39020375,39211011,00.htm>>

<<http://www.securityfocus.com/news/11259>>

<http://hosted.ap.org/dynamic/stories/C/CISCO_SECURITY_CRACKDOWN?SITE=APWEB&SECTION=HOME&TEMPLATE=DEFAULT> oppure <<http://tinyurl.com/8oyxh>>

<<http://news.zdnet.co.uk/0,39020330,39211231,00.htm>>
<<http://www.wired.com/news/politics/0,1283,68356,00.html>>
<http://www.theregister.co.uk/2005/08/02/cisco_exploits/>
<<http://news.zdnet.co.uk/internet/security/0,39020375,39212014,00.htm>>

L'intervista di Wired a Lynn:

<<http://www.wired.com/news/privacy/0,1848,68365,00.html>>

Commenti:

<http://blogs.businessweek.com/the_thread/techbeat/archives/2005/07/the_black_hats.html>
oppure <<http://tinyurl.com/85q74>>
<<http://www.eweek.com/article2/0,1895,1842310,00.asp>>
<http://searchsecurity.techtarget.com/columnItem/0,294698,sid14_gci1112773,00.html?track=NL-358&ad=525032HOUSE> oppure <<http://tinyurl.com/b8u9o>>
<<http://www.computerworld.com/newsletter/0,4902,103634,00.html>>
oppure <<http://tinyurl.com/8kcll>>
<http://searchsecurity.techtarget.com/columnItem/0,294698,sid14_gci1113755,00.html>
oppure <<http://tinyurl.com/dueur>>

I post del blog di Jennifer Granick:

<http://www.granick.com/archive/2005_08_01_theshout_archive.html#112302921362405957>
> oppure <<http://tinyurl.com/bykzw>>
<http://www.granick.com/archive/2005_08_01_theshout_archive.html#112311806179768898>
> oppure <<http://tinyurl.com/8d2ut>>
<http://www.granick.com/archive/2005_08_01_theshout_archive.html#112320079983935922>
> oppure <<http://tinyurl.com/buqfx>>
<http://www.granick.com/archive/2005_08_01_theshout_archive.html#112330515113516813>
> oppure <<http://tinyurl.com/a5emv>>

Un video di Cisco/ISS che strappano pagine dagli atti della conferenza BlackHat:

<http://www.makezine.com/blog/archive/2005/08/video_of_ciscoi.html>

I miei articoli sull'esposizione totale:

<<http://www.schneier.com/crypto-gram-0111.html#1>>
<<http://www.schneier.com/crypto-gram-0203.html#2>> (originale)
<<http://www.cryptogram.it/marzo02.htm#a2>> (traduzione in italiano)

Il mio articolo su segretezza e sicurezza:

<<http://www.schneier.com/crypto-gram-0205.html#1>> (originale)
<<http://www.cryptogram.it/maggio02.htm#a1>> (traduzione in italiano)

Il mio articolo su chiavi e serrature:

<<http://www.schneier.com/crypto-gram-0302.html#1>> (originale)
<<http://www.cryptogram.it/febbraio03.htm#a1>> (traduzione in italiano)

Copie della presentazione di Lynn, o forse una lettera cease-and-desist:

<<http://www.infowarrior.org/users/rforno/lynn-cisco.pdf>>
<<http://www.jwdt.com/~paysan/lynn-cisco.pdf>>
<<http://www.infowarrior.org/users/rforno/lynn-cisco.pdf>>
<<http://www.purpleandgrey.com/free/lynn-cisco.pdf>>
<<http://cryptome.org/lynn-cisco.zip>>
<<http://www.securitylab.ru/Exploits/2005/07/lynn-cisco.pdf>>
<<http://www.jwdt.com/~paysan/lynn-cisco.pdf>>
<<http://files.bitcix.ru/index.php?dir=ebooks/&file=lynn-cisco.pdf>>
<<http://s48.yousendit.com/d.aspx?id=1EOE4MPD1E6U53MYQE6ROJID0R>>
<<http://www.megaupload.com/?d=31GTUIFR>>
<<http://www.dfconsultants.com/lynn-cisco.pdf>>

<<http://www.security.nnov.ru/files/lynn-cisco.pdf>>
<<http://www.mininova.org/get/81889>>
<<http://www.stephencollins.org/library/lynn-cisco.pdf>>
<<http://teknews.net/~radio/lynn-cisco.pdf>>
<<http://snafu.priv.at/download/lynn-cisco.pdf>>

Le fotografie della presentazione vera e propria di Lynn erano qui:

<<http://www.tomsnetworking.com/Sections-article131.php>>

Ora sono qui:

<<http://42.pl/lynn/>>

Qualcuno sta attivando un fondo per finanziare la difesa legale di Lynn. Mandate offerte via PayPal a Abaddon@IO.com (qualcuno conosce l'URL?). Secondo BoingBoing, le offerte che non verranno usate per difendere Lynn saranno donate a EFF.

<http://www.boingboing.net/2005/07/30/mike_lynn_presentati.html>

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

Revoca di una delibera sull'intercettazione di email

Una corte d'appello statunitense ha stabilito che l'intercettazione di e-mail in archivi temporanei è una violazione del wiretap act (legge sull'intercettazione) governativo, revocando il verdetto precedente di un'altra corte.

Sostanzialmente, vi sono leggi sulla privacy differenti che proteggono comunicazioni elettroniche in transito e dati archiviati; le prime sono molto più protette dei secondi. La posta elettronica conservata dal mittente o dal destinatario è ovviamente da considerarsi un insieme di dati archiviati. Ma come inquadrare l'e-mail in viaggio da mittente a destinatario? Da una parte si tratta certamente di comunicazione in transito. Ma il governo ha obiettato che essa in realtà viene di volta in volta archiviata temporaneamente su vari computer mentre transita in Internet: di conseguenza è da trattarsi come insieme di dati archiviati.

La decisione iniziale della corte in questo caso appoggiò il governo. Nel giudizio originale il giudice Lipez scrisse un dissenso molto ispirato. Nella seconda udienza *_en banc_* (con più giudici), egli ha scritto il giudizio per la maggioranza, che ha rovesciato la sentenza precedente.

Il testo del giudizio è lungo, ma ne consiglio caldamente la lettura. È ben articolato e ponderato, e manifesta una comprensione e un'attenzione straordinarie per i dettagli. E una grande chiosa: "Se il problema qui presentato fosse legato al giardinaggio... questo è un giardino che avrebbe bisogno di un diserbante".

Ho contribuito al caso in una breve comunicazione *Amicus Curiae* ("amico della corte").

Qui è sottesa una problematica più grande, ed è la stessa che l'industria dell'intrattenimento ha usato per espandere a dismisura la legge sul copyright nel cyberspazio. Hanno sostenuto che ogni volta in cui un'opera protetta da copyright viene spostata da computer a computer, o da un CD-ROM alla RAM, o da un server a un client, o da hard disk a scheda video, ne viene creata una "copia". Questa ridicola definizione di "copia" ha permesso all'industria dell'intrattenimento di esercitare un controllo legale di gran lunga maggiore sull'utilizzo delle opere protette da copyright.

La decisione:

<http://www.epic.org/privacy/councilman/kerr_amicus.pdf>

Riassunto del caso e delle implicazioni di privacy:

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

La mia breve:

<<http://www.csoonline.com/read/080105/debrief.html>>

Una breve comunicazione da parte di sei diverse organizzazioni per i diritti civili:

<http://www.epic.org/privacy/councilman/kerr_amicus.pdf>

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

Rubare merce immaginaria

È in circolazione un nuovo Trojan che cerca di rubare password di World of Warcraft.

Questo mi ha fatto ricordare di certi individui che pagano dei programmatori per trovare exploit per fare soldi virtuali in giochi multiplayer online, per poi vendere il ricavato in cambio di denaro vero.

Qui c'è una pagina Web che tratta dei sistemi con cui si ruba denaro virtuale nel gioco online Neopets, utilizzando cookie grabber, pagine di login fasulle, falsi concorsi, ingegneria sociale e schemi a piramide.

Da sempre sostengo che ogni forma di furto e frode che esiste nel mondo reale verrà prima o poi riprodotta nel cyberspazio. Forse tutti i metodi per rubare denaro vero un giorno saranno utilizzati per rubare anche denaro immaginario.

<<http://securityresponse.symantec.com/avcenter/venc/data/pwsteal.wowcraft.html>>

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

<<http://www.1up.com/do/feature?cId=3141815>>

<<http://star-girl.org/pages/reads/neopets/avoidscams.php>>

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

Le ristampe di Crypto-Gram

Crypto-Gram è attualmente al suo ottavo anno di pubblicazione. I numeri precedenti coprono tutta una serie di argomenti legati alla sicurezza e si possono trovare a questo indirizzo: <<http://www.schneier.com/crypto-gram.html>>. Quella che segue è una selezione di articoli apparsi in questo mese gli anni scorsi.

"BOB" a bordo:

<<http://www.schneier.com/crypto-gram-0408.html#1>> (originale)

<<http://www.cryptogram.it/cryptogramPdf/Agosto2004.pdf>> (traduzione in italiano)

Gli alibi e la gentilezza degli sconosciuti:

<<http://www.schneier.com/crypto-gram-0408.html#3>> (originale)

<<http://www.cryptogram.it/cryptogramPdf/Agosto2004.pdf>> (traduzione in italiano)

I ranger dell'aeroporto di Houston:

<<http://www.schneier.com/crypto-gram-0408.html#7>> (originale)

<<http://www.cryptogram.it/cryptogramPdf/Agosto2004.pdf>> (traduzione in italiano)

raggio. È una soluzione totalmente inutile se un terrorista si serve di qualcos'altro al posto di un cellulare. Un timer da cucina, per esempio. Ancora peggio, è un danno per la sicurezza nel caso generale. Ma ci siamo dimenticati di come i cellulari hanno salvato delle vite umane durante la tragedia dell'11 settembre? Le comunicazioni avvantaggiano più i difensori che gli aggressori.

<<http://www.nytimes.com/reuters/technology/tech-security-cellphones.html>>

<<http://www.ny1.com/ny1/content/index.jsp?stid=1&aid=52050>>

<<http://www.computerworld.com/mobiletopics/mobile/story/0,10801,103125,00.html>> oppure

<<http://tinyurl.com/72g8h>>

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

Perquisizione delle borse nelle metropolitane

La polizia di New York City inizierà a effettuare perquisizioni casuali delle borse nelle metropolitane, sugli autobus, sui treni dei pendolari e sui traghetti. Altre città hanno aderito all'iniziativa.

Se la scelta è fra perquisizioni casuali e profiling, allora le perquisizioni casuali sono una contromisura di sicurezza più efficace. Ma esistono enormi compromessi per ciò che riguarda la libertà. E non credo che si ottenga molta più sicurezza in cambio. Soprattutto considerando il fatto che i passeggeri sono liberi di non farsi perquisire, lasciando la stazione della metropolitana.

"Okay, ragazzi: qui ci sono i vostri esplosivi. Se uno di voi viene scelto per essere perquisito, lasci la stazione. Poi rientri da un'altra parte, o prenda un taxi ed entri alla stazione successiva".

(A dire il vero, anche se è stato riportato dai media, non ho avuto notizia di nessuno che si sia rifiutato di farsi perquisire e abbia lasciato una stazione).

E non credo nemmeno che le perquisizioni saranno completamente casuali. Penso che gli agenti di polizia che faranno le perquisizioni effettueranno un profiling, perché avviene così.

È un'altra "minaccia da film". È un altro "sistema di sicurezza da pubbliche relazioni". È uno spreco di denaro, riduce sostanzialmente le nostre libertà e non ci renderà affatto più sicuri.

Nota finale: spesso ricevo commenti del tipo "La smetta di criticare tutto e ci dica invece che cosa bisognerebbe fare". La mia risposta è sempre la stessa. L'antiterrorismo è massimamente efficace quando non si lascia andare ad assunzioni arbitrarie in merito ai piani dei terroristi. Si smetta di fare perquisizioni in metropolitana e si spenda il denaro in 1) intelligence e investigazioni, per fermare i terroristi a prescindere dai loro piani, e 2) riposta all'emergenza (emergency response), per ridurre al massimo la dirompenza di un attacco terroristico, a prescindere dai piani dei terroristi. Le contromisure atte a difendere bersagli particolari, o che presumono tattiche specifiche, o che portano i terroristi ad apportare banali modifiche ai loro piani, o che sorvegliano l'intera popolazione per cercare pochi terroristi, sono in larga misura inefficaci e non valgono il denaro speso.

<<http://www.nytimes.com/2005/07/21/nyregion/21cnd-security.html>>

<http://www.washingtonpost.com/wpdyn/content/article/2005/07/21/AR2005072101127_pf.html> oppure <<http://tinyurl.com/aowbf>>

Una guida per il cittadino per rifiutare le perquisizioni nelle metropolitane di New York:

<<http://www.flexyourrights.org/subway/>>

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

Plagio e mondo accademico: un'esperienza personale

Uno scritto pubblicato sul numero di Dicembre 2004 del SIGCSE Bulletin, "Cryptanalysis of some encryption/cipher schemes using related key attack" [Crittanalisi di alcuni schemi di crittografia/cifatura utilizzando attacchi related-key] a nome di Khawaja Amer Hayat, Umar Waqar Anis, e S.Tauseef-ur-Rehman, è identico a uno scritto pubblicato da John Kelsey, David Wagner e il sottoscritto nel 1997.

Si tratta chiaramente di plagio. Le frasi sono state parafrasate o riassunte un poco e sono stati introdotti errori di battitura, ma per il resto è proprio identico. È copiato, con la medesima struttura di sezioni, paragrafi e frasi; persino gli stessi nomi delle variabili matematiche. Presenta le stesse particolarità nel modo in cui vengono citati i riferimenti, e così via.

Abbiamo prodotto due studi sull'argomento; questo è il secondo. Nella loro bibliografia non menzionano nessuno dei nostri due studi. C'è un oscuro riferimento a "[KSW96]" nel testo dell'introduzione e dei propositi dello studio, presumibilmente copiato dal nostro testo; ma una citazione completa di "[KSW96]" non è presente nella loro bibliografia. Forse temevano che uno degli esaminatori leggesse gli scritti citati in bibliografia e si accorgesse del plagio.

I tre autori provengono dall'Università Islamica Internazionale di Islamabad in Pakistan. Il terzo autore, S.Tauseef-Ur-Rehman, è un capo di dipartimento (e membro della facoltà) nel dipartimento di Ingegneria delle Telecomunicazioni in questa istituzione pakistana. Se credete alla sua versione, che è probabilmente vera, egli non ha avuto niente a che fare con la ricerca: ha semplicemente aggiunto il proprio nome a uno scritto di due suoi studenti (non è insolito, accade molto spesso nelle università di tutto il mondo). Ma questo non lo toglie dai guai: egli rimane responsabile di qualsiasi cosa su cui metta il proprio nome.

E non siamo gli unici. Gli stessi tre autori hanno plagiato uno studio del crittografo francese Serge Vaudenay e di altri autori. E uno dei lettori del mio blog ha scoperto un terzo studio plagiato, e potenzialmente un quarto.

Ho scritto al direttore del SIGSCE Bulletin, il quale ha eliminato lo studio dal sito Web e ha ordinato lettere ufficiali di ammissione di colpa e di scuse. Hanno detto che proibiranno ai tre autori di presentare altri lavori, ma hanno poi ritrattato. Mark Mandelbaum, direttore dell'ufficio pubblicazioni di ACM, ora sostiene che ACM non ha una linea di condotta specifica per i casi di plagio e che non saranno presi ulteriori provvedimenti. Ho anche scritto a Springer-Verlag, l'editore del mio studio originale.

Non biasimo i periodici per aver pubblicato questi scritti. Sono stato esaminatore di vari studi, ed è praticamente impossibile verificare se l'elaborato di una ricerca sia originale o meno. Siamo noi studiosi, in larga misura, ad autogestirci in merito a una linea di condotta.

Nella maggior parte dei casi il sistema funziona. Questi tre sono stati scoperti e dovrebbero essere licenziati e/o espulsi. Di certo ACM dovrebbe proibire loro di presentare altri scritti, e la loro dichiarazione sul fatto di non avere una linea di condotta specifica per i casi di plagio mi ha lasciato molto sorpreso. Il plagio in ambito accademico è abbastanza grave da permettere questo livello di provvedimenti. Non so però se il sistema funzioni in Pakistan. Spero di sì. Queste persone erano a conoscenza dei rischi quando hanno commesso il plagio. E lo hanno fatto più di una volta.

Se sembro arrabbiato, non lo sono. Sono più che altro divertito. Avevo sentito di ricercatori provenienti da paesi in via di sviluppo che ricorrevano al plagio per infarcire i propri curriculum, ma mi ha sorpreso ritrovarmi vittima di un plagio, davvero. Non sarebbe stato più furbo scegliere un autore meno conosciuto?

E fa piacere sapere che il nostro lavoro è considerato ancora rilevante a distanza di otto anni.

Il mio studio:

<<http://www.schneier.com/paper-relatedkey.html>>

La versione plagiata:

<<http://portal.acm.org/citation.cfm?doid=1041624.1041665>>

Un altro studio:

<http://lasecwww.epfl.ch/php_code/publications/search.php?ref=CHVV03>

La versione plagiata:

<<http://www.ansinet.org/fulltext/itj/itj33327-331.pdf>>

Un terzo studio:

<http://www.iki.fi/vph/files/rtp_security.pdf>

La versione plagiata:

<<http://www.ansinet.org/fulltext/itj/itj33311-314.pdf>>

Le scuse sono in fondo a questa pagina:

<<http://www.schneier.com/paper-relatedkey-p.html>>

Vi è un acceso dibattito, soprattutto da parte di altri studenti dell'Università Islamica Internazionale, nella sezione commenti del post sul mio blog:

<http://www.schneier.com/blog/archives/2005/08/plagiarism_and.html>

E qui alcune notizie sull'accaduto (si noti che il mio nome è scritto in modo totalmente errato):

<<http://www.onlinenews.com.pk/details.php?id=85519>>

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

Rivista la sicurezza dei passaporti RFID

Ho scritto in precedenza in merito ai chip RFID nei passaporti. Due recenti articoli riassumono l'ultima proposta del Dipartimento di Stato, e sembra davvero buona. Stanno cercando di risolvere problematiche di privacy e lo stanno facendo in maniera corretta.

La funzionalità più importante da essi ideata è un sistema di controllo accessi per il chip RFID. I dati nel chip sono criptati, e la chiave è stampata sul passaporto. L'ufficiale fa scorrere il passaporto attraverso un lettore ottico per ottenere la chiave, quindi il lettore RFID la utilizza per comunicare con il chip RFID. Questo significa che il possessore del passaporto può controllare chi ha accesso alle informazioni contenute nel chip; non è possibile che qualcuno possa dare un'occhiata alle informazioni del passaporto senza prima aprirlo e leggere i dati all'interno. Ottima sicurezza.

Il nuovo modello incorpora anche una sottile schermatura radio nella copertura, che protegge il chip quando il passaporto è chiuso. Altra ottima sicurezza.

Se il Dipartimento di Stato implementa queste funzionalità (prevedibilmente, a questo punto), e tali funzionalità funzionano come annunciato (un grande "se", ve lo garantisco), allora non sono più contrario all'idea. E, cosa ancora più importante, avremo un esempio di un sistema di identificazione RFID con ottimi accorgimenti per salvaguardare la privacy. Si dovrebbero rendere obbligatori questi accorgimenti anche per altri documenti d'identità RFID.

<http://www.usatoday.com/travel/news/2005-08-08-electronic-passports_x.htm>
oppure <<http://tinyurl.com/bgclm>>
<http://www.wired.com/news/privacy/0,1848,68451,00.html?tw=wn_tophead_2>

I miei interventi precedenti:

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

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

I rischi legati alla perdita di dispositivi portatili

Con l'aumentare della potenza dei PDA e la diminuzione dei costi della memoria, sempre più persone portano con sé moltissime informazioni personali in un formato che è molto facile smarrire.

L'ho notato per esperienza personale. Se non facessi uno sforzo volontario per limitare la quantità di dati presenti sul mio Treo, questi comprenderebbero informazioni dettagliate sulla mia agenda degli ultimi sei anni. Il mio piccolo computer portatile conserverebbe ogni e-mail che ho inviato e ricevuto negli ultimi dodici anni, e così via. Molti di noi si portano in giro una quantità incredibile di dati molto personali.

Senza dimenticare che molti di noi portano con sé anche dati personali di altre persone.

Vi sono molti modi per gestire questa problematica: tanto per cominciare, protezione con password e crittografia. Più recentemente, alcuni dispositivi di comunicazione, se smarriti, possono essere azzerati a distanza.

<<http://www.washingtonpost.com/wp-dyn/content/article/2005/07/24/AR2005072401135.html>>
oppure <<http://tinyurl.com/drnep>>

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

Come non risolvere il problema dei documenti d'identità

Molti dei terroristi dell'11 settembre possedevano, sotto falso nome, regolari patenti di guida dello stato della Virginia. Non si trattava di documenti contraffatti, ma di documenti d'identità dello stato della Virginia assolutamente validi, che erano stati venduti illegalmente dagli impiegati del Dipartimento della Motorizzazione.

E quindi che cosa ha fatto lo stato della Virginia per risolvere il problema? Ha fatto in modo che ora sia necessaria più burocrazia per ottenere un documento d'identità.

Ma il problema non era la facilità con cui ottenere un documento d'identità. Il problema è che tali documenti venivano venduti illegalmente dagli stessi impiegati statali. Ecco perché la "soluzione" non funziona e il problema rimane:

"Il direttore del Dipartimento della Motorizzazione della Virginia a Springfield Mall è stato accusato di aver venduto patenti di guida a immigrati clandestini e ad altri individui per 3.500 dollari al pezzo.

“L’arresto di Francisco J. Martinez è il secondo caso in due anni a vedere accusato un dipendente del Dipartimento della Motorizzazione della Virginia del Nord di aver venduto illecitamente delle patenti in cambio di denaro. Un caso analogo due anni fa all’ufficio di Tysons Corner del Dipartimento della Motorizzazione della Virginia ha portato alla sentenza di colpevolezza di due impiegati”.

E dopo che si saranno spesi miliardi di dollari per il REAL ID act, e dopo la richiesta di ancor più modulistica per ottenere dei documenti d’identità statali, il problema continuerà ad esistere.

<<http://www.washingtonpost.com/wp-dyn/content/article/2005/07/12/AR2005071201421.html>> oppure <<http://tinyurl.com/cr4w7>>

Requisiti per la patente di guida in Virginia:

<<http://www.dmvnow.com/webdoc/pdf/dmv141.pdf>>

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

Secure Flight

Lo scorso mese il GAO ha pubblicato un nuovo rapporto su Secure Flight. Si esprime in un linguaggio amichevole, ma non promette niente di buono. Ecco un estratto:

“Durante il nostro lavoro di revisione, tuttora in corso, del programma Secure Flight, abbiamo scoperto che la TSA, nelle sue notifiche di privacy dell’autunno 2004, non ha interamente divulgato al pubblico il proprio utilizzo di informazioni personali, come richiesto dal Privacy Act. In particolare, non è stato reso noto al pubblico, né è stato permesso al pubblico di commentare, l’utilizzo da parte della TSA di informazioni personali ricavate da fonti commerciali per testare alcuni aspetti del programma Secure Flight. Nel settembre 2004 e nel novembre 2004, la TSA ha emesso notifiche di privacy nel Registro Federale che includevano descrizioni riguardanti l’uso che sarebbe stato fatto di tali informazioni. Tuttavia queste notifiche non hanno informato completamente il pubblico, prima che la fase di test iniziasse, sulle procedure che la TSA e i suoi appaltatori avrebbero seguito per raccogliere, utilizzare e conservare i dati commerciali. Inoltre, l’ambito e lo scopo dei dati utilizzati durante il test dei dati commerciali non sono stati apertamente divulgati nelle notifiche. Nello specifico, un appaltatore della TSA, agendo per conto dell’agenzia, ha raccolto più di 100 milioni di record di dati commerciali contenenti informazioni personali quali nome, data di nascita e numero di telefono, senza informare il pubblico. Come conseguenza dell’operato della TSA, il pubblico non ha ricevuto la completa protezione garantita dal Privacy Act”.

Capito? La TSA ha violato la legge federale quando stava segretamente estendendo l’uso da parte di Secure Flight dei dati commerciali sui passeggeri. E sulla questione ha mentito al Congresso e al pubblico.

Molto di questo non è nuovo. Lo scorso mese si è saputo che la TSA ha comprato e sta archiviando dati commerciali sui passeggeri, malgrado i funzionari avessero dichiarato che non lo avrebbero fatto e malgrado il Congresso abbia detto loro di non farlo.

Secure Flight è un disastro sotto ogni punto di vista. La TSA ha agito in totale inosservanza della legge e del Congresso. Ha mentito praticamente a tutti quanti. E sta trasformando Secure Flight da semplice programma per confrontare i passeggeri delle linee aeree con watch list antiterrorismo, a complesso programma per compilare dossier sui passeggeri in modo da poter assegnare loro una specie di punteggio indicante le probabilità di essere o meno dei terroristi.

Che è esattamente quel che non doveva essere all’inizio.

Ecco ciò che ho scritto su Secure Flight a gennaio:

“Per chi non ha seguito queste vicende, il programma Secure Flight è il seguito di CAPPS-I (CAPPS sta per Computer Assisted Passenger Pre-Screening). CAPPS-I è entrato in vigore nel 1997, ed è un semplice sistema che confronta i passeggeri delle linee aeree con una watch list di terroristi. Un seguito a questo sistema, CAPPS-II, è stato proposto lo scorso anno. Un sistema più complicato, che avrebbe assegnato a ogni viaggiatore un “punteggio di rischio” basato su informazioni contenute in database governativi e commerciali. Si è levato un incredibile scalpore da parte del grande pubblico, accusando l'eccessiva invadenza del sistema, ed è stato cancellato durante l'estate. Secure Flight è il nuovo sistema a seguito di CAPPS-I”.

A quel tempo, Secure Flight era stato pensato per essere semplicemente un sistema migliore per mettere a confronto i passeggeri delle linee aeree con watch list antiterrorismo.

Faccio parte di un gruppo di lavoro della TSA che sta esaminando le implicazioni di privacy e sicurezza di Secure Flight. Prima di unirmi al gruppo ho dovuto firmare un NDA, cioè un Accordo di Non Divulgazione, accettando di non divulgare alcuna informazione appresa all'interno del gruppo, e di non parlare delle decisioni prese all'interno del gruppo. Ma non c'è ragione di credere che la TSA non stia mentendo al gruppo né più né meno di quanto abbia fatto con il Congresso, e non ho appreso nulla all'interno del gruppo di lavoro che valga la pena discutere. Tutto quel che dico in questa sede proviene da documenti pubblici.

A gennaio ho tracciato alcune conclusioni generali su Secure Flight, e non sono cambiate:

“1) Assumendo che occorra implementare un programma per mettere a confronto i passeggeri delle linee aeree con i nomi di watch list antiterrorismo, Secure Flight è un grande passo avanti -- sotto quasi ogni aspetto -- se comparato a quel che è attualmente in vigore. (E con questo mi riferisco unicamente al programma di confronto, non ai potenziali utilizzi di dati commerciali o provenienti da terze parti).

2) Il sistema di sicurezza che circonda Secure Flight è pieno di buchi di sicurezza. Vi sono problemi di sicurezza legati a documenti d'identità fasulli, alla verifica dei documenti stessi, alla possibilità di volare utilizzando un biglietto aereo altrui, alle procedure delle linee aeree, ecc. Un terrorista ha a disposizione tantissimi modi per aggirare il sistema che non si può considerarlo un sistema sicuro.

3) Il desiderio di applicare questo sistema ad altri ambiti sarà irresistibile. È davvero facile dire: “Visto che avete questo sistema per beccare i terroristi, perché non usarlo con questo elenco di spacciatori di droga... e, già che ci siamo, ci sarebbe anche da pensare all'evento Super Bowl”. Una volta che Secure Flight sarà realizzato, basterà preparare una nuova legge, e avremo un sistema di checkpoint di sicurezza a scala nazionale.

4) Un programma per mettere a confronto i passeggeri delle linee aeree con watch list antiterrorismo non ci rende apprezzabilmente più sicuri, ed è un pessimo modo di spendere i nostri soldi in ambito di sicurezza”.

Quel che è cambiato è il raggio d'azione di Secure Flight. Anzitutto ha iniziato ad utilizzare dati provenienti da fonti commerciali, come Acxiom. Tecnicamente, stanno verificando l'utilizzo di dati commerciali, ma rimane sempre una violazione. Anche il Dipartimento per la Sicurezza Nazionale ha iniziato a investigare la possibile violazione da parte della TSA di leggi federali sulla privacy.

Qual è stata la risposta della TSA dopo essere stata scoperta a violare la sua stessa politica sulla privacy? Modificarla. Un articolo di news cita un funzionario TSA il quale sostiene sia normale modificare dichiarazioni di politica sulla privacy in fase di test.

In realtà non è tanto normale. Ed è meglio cambiare la politica sulla privacy prima di violarne la vecchia versione. Cambiarla a fatto compiuto non è granché bello.

Lo scopo di Secure Flight è quello di confrontare i passeggeri delle linee aeree con elenchi di nominativi di sospetti terroristi. Ma la stragrande maggioranza delle persone segnalate in questo elenco ha semplicemente lo stesso nome o un nome simile a quello del sospetto terrorista. Ted Kennedy e Cat Stevens sono due esempi eccellenti. La questione è se combinare i dati commerciali con il PNR (Passenger Name Record) fornito dalla compagnia aerea possa ridurre questo problema di falsi positivi. Forse conoscere l'indirizzo, o il numero di telefono, o la data di nascita di un passeggero potrebbe ridurre i falsi positivi. O forse no, dipende da quali dati sono inseriti nelle watch list. In ogni caso, fare delle verifiche è sicuramente una cosa sensata.

Ma utilizzare dati commerciali ha delle gravi implicazioni per quanto concerne la privacy, motivo per cui il Congresso ha ordinato tutta una serie di norme intorno ai test della TSA sui dati commerciali, a cui si sono aggiunte altre norme prima che si potesse arrivare a un sistema definitivo. Norme e regole che la TSA ha deciso di ignorare completamente.

I dati commerciali, sotto CAPPS-II, servivano anche ad altro. In quel programma ora defunto, ogni passeggero sarebbe stato sottoposto a un background check computerizzato per determinare il loro essere un "rischio" per la sicurezza aerea. Il sistema avrebbe assegnato un punteggio di rischio basato su dati commerciali: una valutazione del credito, quanto recentemente hanno traslocato, che genere di occupazione avevano, ecc. Questa possibilità è stata eliminata da Secure Flight, ma ora è riapparsa. Un articolo dell'Associated Press porta una dichiarazione di Justin Oberman, il funzionario della TSA responsabile di Secure Flight: "Stiamo cercando di usare i dati commerciali per verificare le identità di chi vola perché non ci affideremo completamente alla watch list... Se ci limitiamo all'ambito della watch list, non è adeguato".

Oberman ha anche testimoniato in un'udienza congressuale:

"THOMPSON: Vi sono un paio di domande, in merito a Secure Flight, a cui mi piacerebbe darvi una risposta. Secure Flight potrà individuare una persona con forte radici comunitarie ma facente parte di una cellula terroristica in attesa, oppure una persona deve essere un terrorista riconosciuto per essere individuato da Secure Flight?

"OBERMAN: Lasci che le risponda in questo modo: il programma identificherà i riconosciuti o sospetti terroristi contenuti nel database di screening antiterrorismo, e dovrebbe essere in grado di identificare persone che potrebbero non trovarsi sulla watch list. Dovrebbe essere in grado di farlo. Oggi non siamo in condizioni di affermare che lo possa fare con certezza, ma riteniamo che sia assolutamente cruciale che sia in grado di farlo.

"E quindi stiamo conducendo questo test dei dati commercialmente disponibili per affrontare proprio tale problematica. È un lavoro molto difficile, in generale. È particolarmente difficile da attuare quando si ha un sistema che trasporta 1,8 milioni di persone al giorno su 30.000 voli in 450 aeroporti. È un ostacolo molto arduo da superare.

"È anche molto difficile da attuare quando si ha a che fare con una minaccia come lei l'ha descritta, ovvero qualcuno che si è in un certo senso mimetizzato nella società e non è così facilmente distinguibile quando entra in un aeroporto. Per questo non mi stancherò di sottolineare quanto crediamo sia importante che il programma possa avere tale funzionalità. Ed è per questa precisa ragione che abbiamo condotto il test con i dati commerciali, che abbiamo esteso il periodo di prova e che siamo molto speranzosi che i risultati siano per noi più che positivi. Così potremo venire qui, spiegarvi e dimostrarvi perché abbiamo bisogno di incorporare quella funzionalità nel sistema".

La mia paura è che la TSA abbia già deciso che andrà a utilizzare i dati commerciali, a prescindere dai risultati dei test. E una volta che si hanno dati commerciali, perché non tracciare

un dossier per ogni passeggero e assegnargli un punteggio di rischio? Allora torniamo a CAPPS-II, proprio il sistema che il Congresso ha annullato la scorsa estate. Anzi, siamo molto vicini a TIA (Total/Terrorism Information Awareness), quel programma di raccolta dati su tutto e tutti che il Congresso ha abolito nel 2003 perché era semplicemente troppo invasivo.

Secure Flight è un pasticcio anche per molte altre ragioni. Un rapporto di marzo del GAO ha dichiarato che Secure Flight non risponde a nove delle dieci condizioni ordinate dal Congresso prima che la TSA potesse spendere denaro sull'implementazione del programma (se non avete letto questo rapporto, posso dire che è piuttosto caustico). Il problema della riparazione del torto (cioè aiutare quelle persone che non possono volare perché hanno lo stesso nome di un terrorista) non sta migliorando. E Secure Flight è in ritardo sulla tabella di marcia e ha già sfornato il budget.

È anche un programma da furfanti che sta operando in flagrante inosservanza della legge. Non può essere eliminato completamente: l'Intelligence Reform e il Terrorism Prevention Act del 2004 richiedono alla TSA di implementare un programma di pre-screening dei passeggeri. E fino a quando non sarà attivato Secure Flight, le compagnie aeree continueranno a confrontare i nomi dei passeggeri con watch list antiterrorismo sotto il programma CAPPS-I. Ma necessita di un serio esame da parte dell'opinione pubblica.

Il rapporto di luglio del GAO:

<<http://www.gao.gov/new.items/d05864r.pdf>>

I miei articoli su Secure Flight:

<<http://www.schneier.com/crypto-gram-0502.html#1>> (originale)

<<http://www.cryptogram.it/Febbraio2005.pdf>> (traduzione)

<<http://www.schneier.com/crypto-gram-0501.html#9>> (originale)

<<http://www.cryptogram.it/Gennaio2005.pdf>> (traduzione)

<<http://www.schneier.com/crypto-gram-0504.html#11>> (originale)

<<http://www.cryptogram.it/Aprile2005.pdf>> (traduzione)

Articoli sulla vicenda:

<<http://www.commondreams.org/headlines05/0621-05.htm>>

<http://www.secondaryscreening.net/static/archives/2005/06/tsa_lies_could.html#000206>

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

<<http://www.airportbusiness.com/article/article.jsp?id=2417&siteSection=5>>

<<http://www.commondreams.org/headlines05/0621-05.htm>>

<<http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2005/07/22/national/w232305D42.DTL>>

oppure <<http://tinyurl.com/dgy4q>>

<<http://www.alternet.org/story/23362/>>

L'udienza congressuale:

<<http://www6.lexisnexis.com/publisher/EndUser?Action=UserDisplayFullDocument&orgId=685&topicId=14299&docId=I:292818506&start=3>> oppure <<http://tinyurl.com/8kz9r>>

Il rapporto di marzo del GAO:

<<http://www.gao.gov/new.items/d05356.pdf>>

Informazioni su Secure Flight:

<<http://www.epic.org/privacy/airtravel/secureflight.html>>

Informazioni su CAPPS-II:

<<http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=13356&c=206>>

Informazioni su TIA:

<<http://www.epic.org/privacy/profiling/tia/>>

che Wells Fargo non offra questo servizio gratuitamente. Anzi, non è vero: è business scaltro per Wells Fargo far pagare il servizio. È riprovevole che il paesaggio legislativo e normativo sia tale che Wells Fargo non avverta che è nel suo miglior interesse offrire questo servizio gratis. Wells Fargo è una società a fini di lucro, e non fa altro che reagire alle realtà di mercato. C'è bisogno che quelle realtà facciano maggiormente l'interesse del pubblico.

<<http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2005/07/22/MNGHADS1TL1.DTL>> oppure
<<http://tinyurl.com/cg6tj>>

Il telefono VOIP criptato di Phil Zimmermann:

<<http://www.wired.com/news/technology/0,1282,68306,00.html>>

Pare che la polizia britannica abbia chiesto al governo una serie di nuovi poteri per combattere il terrorismo, fra cui il diritto di tenere in custodia un sospettato fino a tre mesi senza accusa formale (il limite attuale è di 14 giorni), e rendere infrazione penale il non fornire alla polizia chiavi crittografiche. Quando a Sir Ian Blair è stato chiesto il perché la polizia volesse quell'intervallo di tempo supplementare, egli ha risposto che a volte avevano necessità di accedere a file criptati e che 14 giorni non erano sufficienti per rompere la protezione. Tale risposta non ha senso. Se da un lato è certamente possibile che i programmi per scoprire password abbiano maggiori probabilità di successo avendo tre mesi a disposizione, il RIP (Regulation of Investigatory Powers) Act, che è entrato in vigore nel 2000, già permette alle forze dell'ordine di incarcerare chi non rilascia chiavi crittografiche.

<<http://www.guardian.co.uk/print/0,3858,5245014-117079,00.html>>

<http://edge.channel4.com/news/2005/07/week_4/26_blair.wmv>

<<http://www.guardian.co.uk/theissues/article/0,6512,334007,00.html>>

Intel e Microsoft stanno utilizzando tecnologia DRM per tagliare fuori Linux dal mercato dei contenuti digitali.

<<http://theinquirer.net/?article=24638>>

Il mio articolo sulla piattaforma "Trusted Computing" di Microsoft:

<<http://www.schneier.com/crypto-gram-0208.html#1>> (originale)

<<http://www.cryptogram.it/agosto02.htm#a1>> (traduzione)

Il mio articolo sul monopolio di Microsoft, che ha previsto questo genere di comportamento:

<<http://www.schneier.com/crypto-gram-0310.html#12>> (originale)

<<http://www.cryptogram.it/ottobre03.htm#a12>> (traduzione)

<<http://www.cciinet.org/papers/cyberinsecurity.pdf>>

Affascinante ricerca sulla sorveglianza automatica attraverso telefoni cellulari:

<<http://www.wired.com/news/wireless/0,1382,68263,00.html>>

<<http://reality.media.mit.edu/>>

Microsoft vuole rendere il software piratato meno utile facendo in modo che non possa ricevere patch e aggiornamenti. Allo stesso tempo, è nel miglior interesse di tutti che ogni software sia reso più sicuro, che si tratti di software legale o piratato. Si è parlato di tale questione per un po', e ho trattato in precedenza l'argomento per due volte. Dopo tanto tira-e-molla, Microsoft si è decisa a fare la cosa giusta.

<http://news.com.com/Piracy-check+mandatory+for+Windows+add-ons/2100-1016_3-5804045.html> oppure <<http://tinyurl.com/9d2qw>>

I miei scritti precedenti:

<http://www.schneier.com/blog/archives/2005/02/pirated_windows.html>

<<http://www.schneier.com/crypto-gram-0406.html#4>> (originale)

<<http://www.cryptogram.it/Giugno2004.pdf>> (traduzione)

Hacking ai danni dei sistemi a infrarossi degli alberghi:

<<http://www.wired.com/news/privacy/0,1848,68370,00.html>>

Il Dipartimento per la Sicurezza Nazionale sta testando un programma per emettere carte d'identità RFID ai visitatori che entrano negli Stati Uniti.

<<http://www.thewhig.com/webapp/sitepages/content.asp?contentID=119603&catname=Local+News>> oppure <<http://tinyurl.com/dzm94>>

<<http://www.dhs.gov/dhspublic/display?content=4308>>

Non conosco i dettagli di questo programma né la sicurezza delle carte. In ogni caso, le implicazioni a lungo termine di questo genere di cosa sono agghiaccianti.

Intercettare comunicazioni di automobili compatibili Bluetooth.

<http://trifinite.org/blog/archives/2005/07/introducing_the.html>

<<http://www.computerworld.com/securitytopics/security/story/0,10801,103656,00.html>>

oppure <<http://tinyurl.com/c6qoe>>

Salon ha un articolo interessante sui genitori che si affidano alla tecnologia per controllare i propri figli, invece di controllare altre persone nel loro circondario. Questa è sicurezza basata sulla paura, non sulla ragione. E credo che persone che agiscono in tal modo rendono le proprie famiglie meno sicure.

<<http://www.salon.com/mwt/feature/2005/07/25/gpstrackers/index.html>>

<<http://search.barnesandnoble.com/booksearch/isbnInquiry.asp?isbn=1556524641>> oppure

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

Ecco un rischio post-Guerra Fredda a cui non avevo pensato: scorte di esplosivi nascoste a Mosca:

<<http://www.mosnews.com/feature/2005/07/15/bomba.shtml>>

Sembra che il fenomeno non sia solo sovietico. Negli anni Ottanta e Novanta furono scoperti in Europa Occidentale diverse scorte di armi nascoste dalla CIA e dalla NATO.

Le norme per l'esportazione di crittografia al di fuori degli Stati Uniti sono state rinnovate.

<http://news.com.com/2061-10789_3-5817718.html>

C'è una nuova vulnerabilità di Windows 2000. Quando leggete il testo del link, non lasciatevi sfuggire la spiegazione dai toni sensazionalistici di eEye. Questo è ciò che definisco un "attacco pubblicitario": è un tentativo da parte di eEye Digital Security di ottenere pubblicità per la loro azienda. Certo, sono sicuro che si tratta di una grave vulnerabilità. Certo, sono sicuro che Microsoft avrebbe dovuto fare di più per rendere i propri sistemi più sicuri. Ma anche eEye è da biasimare: è a caccia di vulnerabilità che rendano ottimi comunicati stampa.

<http://news.com.com/Worm+hole+found+in+Windows+2000/2100-1002_3-5817400.html>

oppure <<http://tinyurl.com/9s2p2>>

Il mio articolo sugli attacchi pubblicitari:

<<http://www.schneier.com/crypto-gram-0001.html#KeyFindingAttacksandPublicityAttacks>>

oppure <<http://tinyurl.com/ayvw8>>

L'esempio sbagliato:

<<http://www.schneier.com/crypto-gram-0104.html#2>> (da notare che l'esempio specifico in quell'articolo è sbagliato)

Ecco la vicenda: una donna si trova in una carrozza della metropolitana di Seoul con il suo cane. A un certo punto il cane fa un bisognino sul pavimento. La donna si rifiuta di pulire, malgrado altri passeggeri la invitino a farlo. Qualcuno le scatta una foto, la pubblica su Internet, e la donna riceve il biasimo del pubblico; e la storia rimarrà per sempre in Internet. Poi la blogosfera discute il concetto di Internet come strumento di imposizione sociale.

<http://www.schneier.com/blog/archives/2005/07/dog_poop_girl.html>

Dettagli interessanti sugli ordigni utilizzati nell'attentato di Londra del 7 luglio:

<<http://www.cnn.com/2005/US/08/03/nypd.london.bomb.ap/>>

Per chi di voi è irritato dal fatto che la polizia abbia divulgato la ricetta (acido citrico e decolorante per capelli), i dettagli sono già di dominio pubblico.

<<http://business.fortunecity.com/executive/674/hmtd.html>>

<http://www.fortliberty.org/military-library/Improvised_Primary_Explosives.pdf>

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

<www.roguesci.org/theforum/index.php>

E qui vi sono alcune immagini di esplosivi fatti in casa sequestrati durante i vari raid effettuati dopo gli attentati dinamitardi.

<<http://abcnews.go.com/WNT/popup?id=979901>>

Di solito questo genere di informazioni sarebbero riservate. Pare che la polizia di New York abbia rilasciato tali informazioni per errore.

<http://news.bbc.co.uk/2/hi/uk_news/4746381.stm>

Suonare musica classica sulla soglia del proprio negozio aiuta a prevenire la presenza sgradita di nullafacenti:

<<http://www.freewmexican.com/artsfeatures/10701.html>>

Questa idea è vecchia di almeno dieci anni:

<<http://www.citypages.com/databank/18/842/article3195.asp>>

Si noti che questo non riduce il fenomeno, lo sposta soltanto. Ma se siete il proprietario di un 7-Eleven non vi importa se dei ragazzini vanno a bighellonare al negozio in fondo all'isolato, basta che non lo facciano al vostro negozio.

Un po' di humour sul profiling:

<<http://images.ucomics.com/comics/gm/2005/gm050804.gif/>>

L'Orlando Airport sta guidando un nuovo programma di pre-screening chiamato CLEAR. L'idea è quella di pagare 80 dollari l'anno e di sottoporsi a un background check, e quindi di poter utilizzare una corsia preferenziale al controllo sicurezza negli aeroporti.

<<http://www.airportbusiness.com/article/article.jsp?id=2274&siteSection=5>>

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

<http://www.rednova.com/news/technology/153572/voluntary_airport_security_id_to_debut_in_florida/> oppure <<http://tinyurl.com/9b8ly>>

<<http://www.securityinfowatch.com/online/Biometrics/Orlando-Airport-Debuts-Biometrics-ID-System/4543SIW417>> oppure <<http://tinyurl.com/8f2px>>

<<http://www.flyclear.com/clear.html>>

Ho già scritto in merito a questa idea, fin da quando Steven Brill iniziò per primo a parlarne:

<<http://www.schneier.com/crypto-gram-0403.html#10>> (originale)

<<http://www.cryptogram.it/marzo04.htm#a10>> (traduzione)

Niente di questo programma è diverso da ciò che ho scritto in proposito lo scorso anno. Secondo il loro sito Web: "Il vostro status di membro verrà continuamente esaminato dal corrente programma della TSA, Security Threat Assessment Process (lett. Processo di Valutazione della Minaccia per la Sicurezza). Se il vostro status di sicurezza cambia, lo status associativo verrà disattivato immediatamente e riceverete una email di notifica del cambiamento di status unitamente a un rimborso della parte non utilizzata della quota di associazione annuale". Pensateci. Per 80 dollari l'anno, qualsiasi potenziale terrorista può ricevere automaticamente notifica del fatto che il Dipartimento per la Sicurezza Nazionale lo sta cercando. Bell'affare.

Agli inizi del mese, alla DefCon, un gruppo è stato in grado di impostare una rete 802.11 non amplificata a una distanza di 124,9 miglia (più di 200 chilometri).

<<http://www.enterpriseitplanet.com/networking/news/article.php/3524491>>

<<http://pasadena.net/shootout05/>>

Ancora più importante, il record mondiale di comunicazione con un dispositivo RFID passivo è stabilito a 69 piedi (21,03 metri circa). Ricordatevelo la prossima volta che qualcuno vi dice che è impossibile leggere carte d'identità RFID a distanza.

<http://blogs.washingtonpost.com/securityfix/2005/08/both_black_hat_.html>

<http://www.makezine.com/blog/archive/2005/07/_defcon_rfid_wo.html>

Ogni volta che sentite un costruttore parlare di una limitazione nella distanza di una qualsiasi tecnologia wireless (LAN wireless, RFID, Bluetooth, qualsiasi cosa), partite dal presupposto che abbia torto. Se non ha torto oggi, avrà torto fra un paio d'anni. Date per scontato che qualcuno che investe denaro ed energie per costruire una tecnologia più sensibile possa fare di meglio, e che serviranno meno denaro ed energie nel corso degli anni. La tecnologia migliora sempre, non peggiora mai. Se qualcosa è costoso e difficile oggi, diventerà facile e a buon mercato in futuro.

Questo editoriale di opinione del New York Times sostiene che il panico è in larga misura un mito. Le persone si sentono stressate ma si comportano razionalmente, ed è solo a causa dello stress che si usa il termine "panico".

<<http://www.nytimes.com/2005/08/07/opinion/07fischhoff.html>>

Interessante articolo: "The Hidden Boot Code of the Xbox, or How to fit three bugs in 512 bytes of security code" [Il codice di boot nascosto della Xbox, ovvero come mettere tre bug in 512 byte di codice di sicurezza].

<http://www.xbox-linux.org/wiki/The_Hidden_Boot_Code_of_the_Xbox>

Microsoft voleva tagliare fuori sia i giochi piratati, sia quelli non ufficiali, per cui ha realizzato una "catena di fiducia" (chain of trust) sulla Xbox, dall'hardware all'esecuzione del codice del gioco. Solo codice autorizzato da Microsoft poteva girare sulla Xbox. L'anello di congiunzione di hardware e software in questa catena di fiducia è la boot ROM nascosta "MCPX". L'articolo tratta di questa ROM. Molti errori di sicurezza davvero ingenui.

Un procuratore in Australia ha utilizzato con successo la Difesa MD5 (il fatto che la funzione hash è compromessa) per contrastare un autovelox autostradale.

<<http://theage.com.au/articles/2005/08/10/1123353368652.html>>

<<http://www.news.com.au/story/0,10117,16204811-1242,00.htm>>

Questo è interessante. È vero che MD5 è compromessa. D'altro canto è quasi certamente vero che gli autovelox erano corretti. Se c'è una morale in questa storia, è che la sicurezza teorica è importante nelle azioni legali. Penso sia una buona cosa.

<<http://www.schneier.com/crypto-gram-0409.html#3>> (originale)

<<http://www.cryptogram.it/Settembre2004.pdf>> (traduzione)

Un commento sul fatto che il Governo del Regno Unito sfrutti un insuccesso della sicurezza di frontiera per spingere l'idea di documenti d'identità nazionali:

<http://www.theregister.co.uk/2005/08/04/uk_border_security_analysis/>

Studio sul rilevamento delle impronte digitali:

<http://www.schneier.com/blog/archives/2005/08/fingerprinting_2.html>

Questo potrebbe fare un'enorme differenza nella sicurezza anti-contraffazione. L'idea non è nuova. Ricordo una ricerca sui sistemi anti-contraffazione delle banconote dove venivano aggiunti dei frammenti di fibra ottica alla pasta di cellulosa e veniva presa una "impronta digitale" utilizzando un laser. All'epoca non funzionò, ma era un'idea intelligente.

Checkpoint di sicurezza fai-da-te:

<<http://eurobsd.org/2005-WhatTheHack/reports/markhoekstra-030805/DSC04345.JPG>>

oppure <<http://tinyurl.com/7os5z>>

La TSA vuole che riceviate spam:

<http://www.schneier.com/blog/archives/2005/08/tsa_and_spam.html>

Confessione di un omicidio protetta mediante crittografia:

<http://seattlepi.nwsourc.com/local/aplocal_story.asp?category=6420&slug=ND%20Idaho%20Missing%20Children%20Duncan>

Vi ricordate di tutte quelle storie sui terroristi che nascondevano messaggi nelle trasmissioni televisive? Erano tutti falsi allarmi.

<<http://www.guardian.co.uk/life/feature/story/0,13026,1546179,00.html>>

Il Devil's Infosec Dictionary (Dizionario Infosec del Diavolo):

<<http://www.csoonline.com/read/080105/debrief.html>>

Voglio che sia più divertente. E voglio che la voce che fa riferimento a me ("Crittografia: La scienza di applicare un insieme complesso di algoritmi matematici a dati sensibili allo scopo di

fare Bruce Schneier un uomo incredibilmente ricco”) sia più vera. Sul mio blog sto raccogliendo definizioni migliori e più spiritose. Dite la vostra se volete:

<http://www.schneier.com/blog/archives/2005/08/the_devils_info.html>

NEWS DELL'ULTIM'ORA: Wired News riporta che il Dipartimento per la Sicurezza Nazionale sta facendo pressioni per permettere a Secure Flight di utilizzare database commerciali, e per ridurre la supervisione indipendente del Congresso sul programma.

<http://www.wired.com/news/privacy/0,1848,68518,00.html?tw=wn_tophead_1>

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

Sparare per uccidere

La Polizia Metropolitana di Londra ha una linea di condotta "sparare per uccidere" in caso di sospetti terroristi suicidi. E anche l'International Association of Chiefs of Police ha pubblicato nuove linee guida che consigliano una linea di condotta "sparare per uccidere". La teoria è che solo un colpo diretto alla testa ucciderà immediatamente il terrorista, e quindi annullerà la possibilità di esecuzione di un attacco dinamitardo.

Quali sono gli elementi su cui un agente di polizia si deve basare per ritenervi dei terroristi suicidi, e quindi spararvi alla testa?

"Il profilo comportamentale dell'organizzazione di polizia sostiene che un tale soggetto può mostrare 'molteplici anomalie', fra cui indossare un pesante cappotto o giaccone in una giornata calda o avere con sé una valigetta, una sacca o uno zaino con protuberanze o fili in vista. Il soggetto potrebbe manifestare nervosismo, fuggire lo sguardo altrui, o sudare eccessivamente. Potrebbero esserci delle bruciature chimiche sui vestiti o macchie sulle mani. Il soggetto potrebbe recitare preghiere a mezza voce o 'camminare avanti e indietro di fronte a un luogo di ritrovo'".

Ciò che viene richiesto è tutto qui?

"Le linee guida della polizia dicono inoltre che la minaccia per gli agenti non deve essere necessariamente 'imminente', come insegna tradizionalmente l'addestramento in polizia. Gli agenti non devono aspettare che un sospetto dinamitardo faccia una qualche mossa (altro tradizionale requisito che permette alla polizia di fare uso di forza mortale). Basta che un agente abbia 'basi ragionevoli' per credere che il sospettato possa far brillare un ordigno, dicono le linee guida".

Questa linea di condotta è basata sull'assunzione estremamente miope secondo cui un terrorista debba premere dei pulsanti per detonare una bomba. Infatti, fin dalla Prima Guerra Mondiale, il tipo di ordigno più comune indossato da una persona è stata la bomba a mano. È assolutamente concepibile, soprattutto se si sa che è in atto una linea di condotta "sparare per uccidere", che i terroristi suicidi utilizzeranno per i loro ordigni lo stesso tipo di detonatore a uomo morto, cioè un detonatore che viene attivato quando un pulsante viene rilasciato e non premuto. Questo è un caso difficile. Qualsiasi linea di condotta si scelga, i terroristi si adatteranno e dimostreranno che è quella sbagliata.

Si tratta poi di una linea di condotta che mette a rischio le persone, invece di renderle più sicure. La domanda di sicurezza non è: 'Che altri sistemi possiamo usare per fermare un dinamitardo suicida?'. La vera domanda è: 'Quando la polizia sospetta qualcuno di essere in grado di far saltare una bomba, che cosa dovrebbe fare?'. Dinamitardi che usano zaini sono molto rari, al punto che chiunque sia sospettato dalla polizia molto probabilmente risulterà innocente.

La polizia di Londra è dispiaciuta di aver ucciso per errore un innocente sospettato di essere un dinamitardo suicida, ma posso certamente comprendere lo sbaglio. Alla fine, la soluzione migliore è addestrare gli agenti di polizia e poi lasciare a loro la decisione. Ma in tutta onestà sono preferibili delle linee di condotta che abbiano come risultato l'incarcerazione di sospettati ancora vivi, piuttosto che linee di condotta che producano solo cadaveri, soprattutto quando si scoprirà che molti dei sospettati erano innocenti.

La linea di condotta della polizia di Londra:
<http://news.bbc.co.uk/2/hi/uk_news/4707781.stm>

La linea di condotta della International Association of Chiefs of Police:
<<http://www.washingtonpost.com/wp-dyn/content/article/2005/08/03/AR2005080301867.html>> oppure <<http://tinyurl.com/acmd9>>

** **

Le News di Counterpane

WiTel Communications ora fornisce ai propri clienti i managed services di Counterpane:
<<http://www.counterpane.com/alliances-news.html>>

Schneier è stato intervistato in Government Technology:
<<http://www.govtech.net/magazine/story.php?id=95671>>

** **

Visa e American Express abbandonano CardSystems

Vi ricordate di CardSystems Solutions, la società che ha esposto più di 40 milioni di identità a potenziali frodi? (Il reale quantitativo di persone che saranno effettivamente vittima di frodi è quasi sicuramente molto molto minore).

Sia Visa che American Express stanno abbandonando questa società, eliminandola dai loro payment processor: "A poche ore dall'annuncio che Visa era alla ricerca di un rimpiazzo per CardSystem Solutions, American Express ha dichiarato martedì che cesserà i rapporti di affari con tale società a partire da ottobre".

Il problema maggiore dell'operato di CardSystems non era che la società avesse pessime pratiche di sicurezza informatica, ma che avesse pessime pratiche di affari. Stava trattenendo file contenenti informazioni personali, e non doveva farlo. Non era a scopo di marketing, come ho sospettato in origine, ma per determinare perché le transazioni non venivano autorizzate. Era in piena inosservanza delle norme che aveva accettato di seguire.

Si può porre rimedio a problemi di ordine tecnico. Una cultura aziendale disonesta è più difficile da sistemare. È ciò che avverto leggendo fra le righe:

"Visa ha ponderato la decisione per alcune settimane, ma a metà giugno scorso aveva dichiarato di stare lavorando con CardSystems per sistemare il problema. CardSystems ha assunto questo mese un verificatore di sicurezza esterno per esaminare le proprie linee di condotta e le proprie pratiche, e ha promesso di effettuare ogni aggiornamento necessario per la fine di agosto. CardSystems, nella sua dichiarazione di ieri ha affermato che i dirigenti della società sono stati 'in contatto pressoché quotidiano' con Visa sin dal momento in cui fu scoperto il problema a maggio.

"Visa, tuttavia, ha dichiarato che malgrado 'alcuni tentativi di rimediare alla situazione' compiuti dal momento in cui è stato riportato l'incidente, l'operato di CardSystems non è stato sufficiente".

E questo:

"CardSystems Solutions Inc. 'non ha risolto, e non può a questo punto risolvere, il fallimento nel fornire un'adeguata sicurezza dei dati per i conti Visa", ha dichiarato Rosetta Jones, un portavoce della sede Visa di Foster City, California ...

"Visa ha dichiarato che, malgrado CardSystems abbia effettuato azioni di rimedio da quando è stata divulgata la fuga di dati, tali azioni non hanno potuto prevalere sul fatto che la società stesse trattenendo inopportuno delle informazioni sui conti, apparentemente per 'motivi di ricerca', quando è avvenuta la fuga di dati, in violazione delle norme di sicurezza di Visa".

A questo punto non è chiaro che cosa faranno MasterCard e Discover.

"MasterCard International Inc. sta manifestando una diversa linea di condotta nei confronti di CardSystems. La compagnia di carte di credito si aspetta da CardSystems lo sviluppo di un piano per migliorare la sua sicurezza, entro il 31 agosto, 'e a tutt'oggi non siamo a conoscenza di alcuna mancanza nei loro sistemi che non possa essere sistemata', ha dichiarato il portavoce Sharon Gamsin.

"Tuttavia, se entro quella data CardSystems non sarà in grado di dimostrare di essere in piena conformità, la possibilità da parte loro di fornire servizi ai titolari MasterCard sarà a rischio", ha aggiunto Gamsin.

"Jennifer Born, una portavoce di Discover Financial Services Inc., anch'essa in relazione d'affari con CardSystems, ha dichiarato che la società di Riverwoods, Illinois, 'sta compiendo i dovuti controlli e prenderà una decisione al termine di tale processo'".

Ritengo che questo sia uno sviluppo positivo. È da molto che dico che società come CardSystems non si comporteranno correttamente finché non ci saranno conseguenze da pagare per non aver seguito le regole. Le compagnie di carte di credito che abbandonano CardSystems stanno mandando un messaggio forte e chiaro agli altri payment processor: migliorate la vostra sicurezza se volete rimanere in affari.

Gli articoli sulla vicenda:

<<http://www.ajc.com/news/content/business/0705/20bizcardsystems.html>>

<<http://www.nytimes.com/2005/07/19/business/19visa.html?adxnnl=1&oref=login&adxnnlx=1121913372-DMgsxuIkCLIs0Cz84OcAlw>> oppure

<<http://tinyurl.com/ax4qa>>

<http://news.yahoo.com/news?tmpl=story&cid=528&e=3&u=/ap/20050720/ap_on_bi_ge/credit_cards_breach> oppure <<http://tinyurl.com/bau3s>>

Il mio articolo originale su CardSystems:

<<http://www.schneier.com/crypto-gram-0507.html#3>> (originale)

<<http://www.cryptogram.it/Luglio2005.pdf>> (traduzione)

Alcune interessanti giudizi legali sulla problematica più ampia della divulgazione:

<<http://writ.news.findlaw.com/ramasastry/20050713.html>>

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

Commenti dei lettori

Da: Ed Gerck <egerck@nma.com>
Oggetto: Commento all'articolo su CardSystems

Come da lei riportato, le compagnie di carte di credito possono obbligare, e lo fanno, le società che processano dati delle carte di credito ad aumentare la propria sicurezza. Che dire, tuttavia, del concetto di "rischi accettabili" che sta alla base delle stesse procedure di sicurezza di queste stesse compagnie di carte di credito?

Il piccolo grande segreto dell'industria delle carte di credito è che le compagnie sono ben contente di quel 10% di frodi ai danni delle carte di credito, che avvengano via Internet o meno.

Infatti, se riducessero il tasso di frode a zero oggi, le loro entrate e i loro profitti diminuirebbero. Per cui non esiste un vero e proprio incentivo a ridurre le frodi. Al contrario, mantenere l'attuale stato di cose va benissimo.

E questo a causa dell'assicurazione: fino a un certo livello, che è largamente all'interno dei limiti operativi, ovvio, una transazione fraudolenta non rimane insoluta attraverso i server di Visa, American Express o MasterCard. La transazione viene pagata interamente, con i relativi costi assicurativi pagati dal commerciante e, in ultima analisi, dal cliente.

"Rischi accettabili" è stato per molto tempo un eufemismo di quel modello di business che sposta il fardello della frode sulle spalle del cliente.

Così l'industria delle carte di credito ha trasformato con successo la frode in una vendita. È lo stesso atteggiamento riferitomi dal rappresentante di una marca di automobili mentre gli stavo parlando di alcune semplici tecniche per ridurre i furti d'auto. La sua risposta è stata: "Un'auto rubata è un'auto venduta".

Infatti un'auto rubata avrà bisogno di essere sostituita, grazie all'assicurazione o dal cliente stesso che si comprerà un'auto nuova col frutto del suo lavoro, mentre la macchina rubata continuerà a generare entrate per il costruttore in termini di servizio e pezzi di ricambio.

Ogni volta che assistiamo a una frode continuata, dovremmo essere certi di una cosa: il defraudato ne sta ricavando dei profitti, perché nessuna azienda accetterebbe una perdita continuata senza fare nulla per ridurla. Argomentazioni quali "non vogliamo ridurre il livello di frode perché costerebbe di più ridurre la frode di quanto costa la frode stessa" sono solo un modo commerciale di affermare che la frode è diventata una vendita.

Perché la frode è un'emorragia in continuo aumento, mentre gli sforzi per ovviare al problema, se messi in opera correttamente, sono in sostanza un costo anticipato che viene affrontato solo una volta. Quindi, accettare debiti dovuti a frode significa accettare anche l'esistenza di un credito che va a compensare il debito continuamente. Il quale credito, in ultima analisi, parte dal cliente. Proprio come con il furto d'auto.

Che cosa biasimare? Non soltanto l'etica distorta che sta dietro questo atteggiamento, ma anche quella tradizionale scuola di pensiero di sicurezza che si focalizza sul rischio, sulla sorveglianza e sull'assicurazione come soluzione ai problemi di sicurezza.

Non vi è alcuna considerazione di ciò che significherebbe davvero la fiducia in termini di bit e macchine, nessuna considerazione che il modello di sicurezza basato sull'assicurazione non può essere scalabile ai livelli di Internet e non può nemmeno essere eticamente giustificabile.

"Una frode è una vendita" è il solo risultato possibile che deriva dal mettere in pratica tale scuola di pensiero di sicurezza. Che a volte prende il nome di "rischi accettabili": accettabili davvero, visto che sono pagati.

Da: Tom Welsh <tom@draco.demon.co.uk>
Oggetto: Re: Ordigni esplosivi improvvisati in Iraq

"In seguito le truppe USA sono diventate esperte nell'individuare e uccidere chi faceva brillare le bombe".

Beh, sì... più o meno. Ci pensi un attimo, ed è facile immaginare come vanno queste cose. "Se una bomba esplode mentre stiamo guidando per strada, fate fuori tutti gli haji che vi sembra stiano tenendo in mano un detonatore a distanza". Bam bam bam! Addio a decine di civili locali, molti dei quali stavano controllando i propri cellulari, o leggendo libri, o tirando fuori dei soldi dal portafoglio, ecc.

Naturalmente questo è ciò che stanno cercando di ottenere gli insorgenti. Uccidere gli infedeli va bene, ma non è l'obiettivo principale. L'obiettivo è fare in modo che gli infedeli uccidano i civili, e diamine se lo fanno, se ben imbrogliati.

Non so se è stato il Vietnam o Mogadiscio a essere il punto di svolta, ma a un certo punto il Pentagono ha deciso che doveva essere ferito il numero più ridotto possibile di ragazzi americani mentre si trovavano a sistemare le sorti del mondo in qualche paese straniero. Metti in mano a un po' di truppe l'armamentario più potente che dei soldati abbiano mai avuto a propria disposizione, di' loro di essere sicuri e di cercare per primi la rappresaglia (come se avessero bisogno di incoraggiamento) e indovina che succede? Pochissimi morti fra le truppe americane, decine di migliaia di civili morti o mutilati, e un tasso di popolarità che si sta avvicinando sempre più a quello delle Waffen-SS. Diamogli ancora un po' di tempo e arriveranno a quello delle Allgemeine-SS.

La mia opinione è che, dal punto di vista di un esperto di sicurezza, sia possibile vincere le battaglie e perdere la guerra. E far fuori qualsiasi "persona dall'aria sospetta" è un modo eccellente per farlo.

Da: Les Jones <llj@sses.net>
Oggetto: RE: CRYPTO-GRAM, 15 luglio 2005

"Questo consiglio avrebbe aiutato Brennan Hawkins, il ragazzino di 11 anni disperso per quattro giorni nel deserto dello Utah il mese scorso. Egli evitava le persone che lo cercavano perché gli era stato insegnato di non parlare agli sconosciuti".

Evitare i soccorritori è una reazione comune in chi si è perduto nei boschi. Si veda il libro di Dwight McCarter, "Lost" (Perduto), un resoconto di operazioni di ricerca e soccorso nel Great Smoky Mountains National Park. In un capitolo McCarter racconta la storia di due escursionisti che nel parco si sono separati mentre camminavano fuori dal sentiero nelle vicinanze di Thunderhead. L'escursionista meno esperto si è subito perduto.

Dopo un giorno o due a vagare senza meta, frugando nel suo zaino, ha trovato un vademecum per escursionisti che spiegava cosa fare in caso ci si trovasse sperduti nei boschi. Seguendo i consigli, si è diretto verso una radura e ha realizzato un fuoco di segnalazione. Un elicottero di soccorso ha notato il fumo ed è sceso a livello degli alberi, mentre l'escursionista agitava le braccia per attirare l'attenzione. L'elicottero ha rilasciato un sacco a pelo e del cibo, con una nota che diceva che non era possibile per loro atterrare nella radura, ma che avrebbero inviato un gruppo di soccorso a piedi.

L'escursionista sperduto si è seduto, ha curato il fuoco, e ha atteso i soccorsi. Quando i soccorritori sono comparsi al limite della radura, in un attacco di panico l'escursionista si è

alzato di scatto ed ha incominciato a correre nella direzione opposta. Hanno dovuto inseguirlo per soccorrerlo. Questo malgrado il fatto che fosse lui a voler essere soccorso, che avesse effettuato tutta una serie di azioni deliberate per attirare i soccorritori e che sapesse che i soccorritori stavano arrivando. Strano ma vero.

Da: Tamas K Papp
Oggetto: Re: Parlare agli sconosciuti

Lei sostiene che "non parlare mai con gli sconosciuti" sia uno dei consigli peggiori che si possano dare a un bambino".

La "politica di sicurezza" del non parlare agli sconosciuti in realtà racchiude due situazioni distinte:

(A) Non iniziare una conversazione con sconosciuti.

(B) Non rispondere se degli sconosciuti cercano di parlarti.

In (A) abbiamo a che vedere con la probabilità a priori (per esempio la loro proporzione rispetto alla popolazione della zona, ecc.) di sconosciuti che possono essere innocui o pericolosi ($p(H)$ e $p(D)$ rispettivamente). Sono d'accordo con la sua conclusione secondo cui in qualsiasi società normale il numero di $p(D)$ è assai ridotto, e quindi in questo caso il consiglio dei genitori un po' paranoici non ha molto senso.

Tuttavia, un'attenta analisi di (B) mostra che qui abbiamo a che vedere con la probabilità a posteriori di sconosciuti pericolosi _considerato il fatto_ che hanno iniziato la conversazione (lo indicheremo con la lettera T). Per calcolare questo si può ricorrere alla Regola di Bayes:

$$p(D|T) = p(T|D)p(D)/p(T)$$

dove $p(T) = p(T|D)p(D) + p(T|H)p(H)$ è la probabilità che sconosciuti di ogni tipo possano parlarti. In una società dove le persone "normali" non parlano agli sconosciuti, $p(T|H)$ è vicino allo zero, mentre è possibile che persone pericolose (chi molesta i bambini, criminali, ecc.) parlino ai bambini con grande probabilità, per cui $p(T|D)$ sarà maggiore di zero.

Perciò, anche se $p(D)$ è un numero basso, $p(D|T)$ può essere sufficientemente alto affinché la parte (B) abbia senso: si sfrutta l'informazione del segnale per rivedere il proprio giudizio in merito alla pericolosità degli sconosciuti.

I genitori possono ritenere la distinzione fra (A) e (B) troppo sottile per la mente di un bambino, e quindi ricorrono alla meno eccellente e più semplice regola di non parlare agli sconosciuti.

Sono d'accordo con lei quando afferma che "In un mondo dove le brave persone sono molte e i malintenzionati una minoranza, presumere che un qualsiasi sconosciuto sia una brava persona è una strategia di sicurezza intelligente". Tuttavia, ignorare i segnali che aiutano a rivedere le proprie valutazioni delle probabilità è una pessima strategia di sicurezza.

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

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

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

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

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

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

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

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

Copyright (c) 2005 by Bruce Schneier.