

CRYPTO-GRAM
15 aprile 2006

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

Edizione italiana curata da Communication Valley SpA

E-mail: schneier@counterpane.com

Web: <http://www.schneier.com> 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>.

Crypto-Gram è anche consultabile in formato RSS.

** **

In questo numero:

Concorso: Minaccia da Trama Cinematografica
Lo screening dei passeggeri delle linee aeree
80 telecamere per 2.400 persone
Le ristampe di Crypto-Gram
Crittografia per VOIP
Sicurezza mediante richieste formali
Il Privacy and Integrity Report del Dipartimento per la Sicurezza Nazionale
News
KittenAuth
I rischi di tipo terroristico di Google Earth
Un nuovo tipo di serratura
Le News di Counterpane
Aggirare il copyright mediante XOR
iJacking
Screening di sicurezza per gli elicotteri di New York
Commenti dei lettori

** **

Concorso: Minaccia da Trama Cinematografica

NOTA: Se avete un blog, vi prego di diffondere l'iniziativa.

È ormai da un certo tempo che scrivo a proposito della nostra passione per le "minacce da trama cinematografica": paure di atti terroristici basate su scenari di attacco molto specifici. Terroristi muniti di pesticidi, terroristi che fanno esplodere passeggeri in metropolitana, terroristi che riempiono di esplosivo gli scuolabus, ecc.: queste sono minacce da trama cinematografica. Sono ottime per spaventare la gente, ma è semplicemente un'idiozia realizzare procedure di sicurezza nazionale per fronteggiarle.

Ma se ci dobbiamo preoccupare di attacchi improbabili, perché non possono essere anche intriganti e innovativi? Se gli americani devono essere terrorizzati, perché non esserlo per cose davvero spaventose? "Far saltare in aria il Super Bowl" è di sicuro da trama di un film, ma non di un buon film. Cerchiamo di aumentarne la qualità.

È in tale spirito che annuncio solennemente il (forse Primo) Concorso: Minaccia da Trama Cinematografica. I partecipanti sono invitati a presentare i più improbabili, però sempre plausibili, scenari di attacco terroristico che possono inventarsi.

Il vostro obiettivo: provocare terrore. Fare in modo che non passi inosservato dai cittadini americani. Infliggere danni profondi e duraturi all'economia statunitense. Cambiare l'assetto politico o la cultura. Più ambizioso risulta l'obiettivo, meglio è.

Presupporre un profilo di aggressore nell'ordine dell'11 settembre: da 20 a 30 persone senza addestramento particolare, e circa 500.000 dollari con i quali comprare esperienza, attrezzature, ecc.

Pubblicare le vostre trame cinematografiche qui su questo blog.

La valutazione sarà a opera mia, con l'influenza del generale entusiasmo nella sezione commenti del blog. Il premio consisterà in una copia autografata di "Beyond Fear". E se mi sarà possibile, una telefonata in diretta con un vero produttore cinematografico.

Il termine di partecipazione è la fine del mese, il 30 aprile.

Non si tratta di un Pesce d'Aprile, anche se è nello spirito della stagione. Il fine di questo concorso è fare dell'assurdo umorismo, ma spero anche che serva a dimostrare qualcosa. Il terrorismo è una minaccia reale, ma misure di sicurezza che ci obbligano a indovinare correttamente quale sarà la prossima mossa dei terroristi non ci rendono affatto più sicuri.

Buona fortuna.

Pubblicate le vostre entrate, e leggete quelle altrui, in questa pagina: http://www.schneier.com/blog/archives/2006/04/announcing_movi.html

Le minacce da trama cinematografica: <http://www.schneier.com/essay-087.html>

<http://www.time.com/time/nation/article/0,8599,175951,00.html>
http://www.schneier.com/blog/archives/2005/10/exploding_baby.html
http://www.schneier.com/blog/archives/2006/02/school_bus_driv.html
<http://www.imdb.com/title/tt0075765>

Qui vi sono centinaia di idee: <http://cockeyed.com/citizen/terror/plans/terrorwatch.html>

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

Lo screening dei passeggeri delle linee aeree

Sembra proprio che ogni volta che la sicurezza aeroportuale viene messa alla prova, questa fallisca. Nei test condotti fra novembre 2001 e febbraio 2002, gli agenti di sicurezza si sono lasciati sfuggire il 70% dei coltelli, il 30% delle pistole e il 60% degli ordigni (fasulli). E di recente chi si è occupato dei test è riuscito a far passare parti di

ordigni esplosivi attraverso i checkpoint dell'aeroporto in 21 tentativi su 21. C'è da chiedersi perché bisogna mettere i computer portatili in una vaschetta separata e togliersi le scarpe (anche se dovremmo tutti ringraziare Richard Reid per non essere stato il "bombarolo della biancheria intima").

Il mancato riconoscimento di parti per costruire bombe è più semplice da comprendere. Basta smontare qualcosa in parti sufficientemente piccole, e passerà le verifiche di sicurezza al checkpoint con estrema facilità. Il materiale esplosivo non verrà rilevato dal metal detector, e le parti elettroniche associate possono apparire innocue quando vengono disassemblate. Questo non è nemmeno un problema nuovo: è largamente ritenuto possibile che le donne cecene che fecero saltare i due aerei russi nell'agosto 2004 introdussero a bordo i loro ordigni smontati in parti.

Ma pistole e coltelli? Questo, senza dubbio, sorprende molte persone.

Gli screener di un aeroporto hanno un compito difficile, in primo luogo perché il cervello umano non si adatta naturalmente al compito stesso. Siamo concentrati sul confronto di pattern visivi, e ce la caviamo molto bene a distinguere ciò che sappiamo di dover cercare, per esempio un leone in un mare di erba alta.

Ma siamo molto meno esperti nell'individuare le eccezioni casuali all'interno di un insieme uniforme di dati. Di fronte a una serie infinita di oggetti identici, il cervello finisce col ritenere identica qualunque cosa e quindi non ha più senso prestare attenzione. Quando infine appare l'eccezione, il cervello semplicemente non la nota. Tale fenomeno psicologico non è soltanto un problema dello screening negli aeroporti: è stato individuato in ogni genere di ispezioni, ed è la ragione per cui i casinò cambiano frequentemente i mazzieri. I compiti sono semplicemente tali da intorpidire la mente.

A peggiorare le cose, l'aggressore può provare a sfruttare la debolezza del sistema, posizionando le armi nel proprio bagaglio in maniera del tutto normale, tentando di occultarle aggiungendo altri oggetti metallici per distrarre gli screener. Può smantellare parti di un ordigno in modo tale da non sembrare affatto quel che sono. Di fronte a uno screener annoiato egli si trova ad avere un grande vantaggio.

Inoltre, come è stato più volte fatto notare in articoli sulla risibilità della sicurezza aeroportuale post-11 settembre, le armi improvvisate rappresentano un enorme problema. Un sasso, la batteria di un computer portatile, una fibbia, la maniglia estensibile di un trolley, il filo da pesca, le mani nude di una persona che pratica il karate... la lista è lunghissima.

La tecnologia può essere di aiuto. Le macchine a raggi X già inseriscono bagagli "di prova" nel flusso per mantenere vigili gli screener. Schermi computerizzati aiutano gli screener a trovare oggetti di contrabbando nel bagaglio, e presto i computer saranno in grado di svolgere la maggior parte del lavoro. Ed è una cosa sensata: in fin dei conti i computer sono eccellenti nell'affrontare compiti noiosi e ripetitivi. Si dovrebbero occupare dello smistamento veloce e lasciare che gli screener si occupino delle eccezioni.

Certo, vi saranno molti falsi allarmi, e qualche oggetto pericoloso riuscirà egualmente a passare, ma è migliore delle alternative.

E forse può risultare sufficientemente efficace. Si ricordi lo scopo dello screening dei passeggeri. Non stiamo cercando di acciuffare quei terroristi furbi, organizzati e ben finanziati, ma i dilettanti e gli

incompetenti. Stiamo cercando di prendere gli instabili, gli imitatori. Sono tutte valide minacce in ogni caso, ed è una cosa intelligente difendersi da esse. Contro i professionisti è semplicemente un tentativo di aggiungere un grado sufficiente di incertezza nel sistema in modo da spingerli verso altri bersagli.

Gli obiettivi dei terroristi non hanno nulla a che vedere con gli aerei; i loro obiettivi mirano a provocare terrore. Far saltare un aereo è soltanto un tipo particolare di attacco allo scopo di raggiungere quell'obiettivo. Gli aerei necessitano di ulteriori misure di sicurezza poiché possiedono caratteristiche che li rendono soggetti a guasti catastrofici: basta una piccola esplosione, e tutti gli occupanti di un aereo muoiono. Ma vi è un rendimento decrescente sugli investimenti in sicurezza aerea. Se i terroristi spostano il bersaglio dagli aerei ai centri commerciali, non abbiamo realmente trovato una soluzione al problema.

Ciò significa che uno screening di base e non particolarmente approfondito è più che sufficiente. Se io dovessi investire in sicurezza, finanzierei una ricerca significativa in attrezzature di screening con l'ausilio di computer, sia per i bagagli fatturati che per quelli a mano, ma non investirei molto denaro in procedure di screening invasive e in screening secondari. Preferirei di gran lunga avere personale di sicurezza ben addestrato che pattugli l'aeroporto, sia in divisa che in borghese, attento a individuare comportamenti sospetti.

Quando viaggio in Europa, non devo mai estrarre il mio portatile dalla custodia né togliermi le scarpe. I governi dell'Unione Europea hanno avuto molta più esperienza con il terrorismo rispetto al governo statunitense, e capiscono bene quando lo screening dei passeggeri ha raggiunto il rendimento decrescente. (Hanno anche implementato misure di sicurezza per il bagaglio fatturato con decenni di anticipo rispetto agli Stati Uniti, ancora una volta riconoscendo la vera minaccia).

E se stessi investendo in sicurezza, investirei in intelligence e nell'investigazione. Il momento migliore per combattere il terrorismo è prima che il terrorista cerchi di imbarcarsi su un aereo. Le contromisure migliori hanno un valore a prescindere dalla natura della trama terroristica o del particolare bersaglio dei terroristi,

In un certo senso, se ci affidiamo agli screener degli aeroporti per prevenire il terrorismo, allora è già troppo tardi. Dopotutto, se non siamo nemmeno in grado di tenere le armi fuori dai penitenziari, come possiamo sperare di tenerle fuori dagli aeroporti?

<http://archives.cnn.com/2002/US/03/25/airport.security/>

<http://www.msnbc.msn.com/id/11863165/>

<http://www.msnbc.msn.com/id/11878391/>

Una versione di questo articolo è originariamente apparsa su Wired.com:

<http://www.wired.com/news/columns/0,70470-0.html>

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

80 telecamere per 2.400 persone

La sperduta cittadina di Dillingham, Alaska, è probabilmente la più vigilata del paese. Vi sono 80 telecamere di sorveglianza per i suoi 2.400 abitanti, ovvero una telecamera ogni 30 persone.

Suppongo che le telecamere siano state acquistate perché il comune non

sapeva in quale altro modo impiegare i 202.000 dollari stanziati dal Dipartimento per la Sicurezza Nazionale (uno dei problemi dello stanziamento di fondi basato su un'agenda di priorità politiche e non su dove siano presenti le minacce vere e proprie).

In ogni caso la città ha ricevuto il denaro, e lo ha speso. E ora deve giustificare la spesa. Ecco la "minaccia da trama cinematografica" usata dal Capo della Polizia di Dillingham per motivare l'efficacia dell'investimento:

"'Il confine con la Russia si trova a 800 miglia da qui in quella direzione', dice puntando il braccio a destra.

"'Seattle si trova a circa 1.200 miglia in quest'altra direzione'. E indica dietro di sé.

"'Per cui, se ho fatto bene i conti, siamo più vicini alla Russia che non a Seattle'.

"'Adesso immaginate', continua: 'Che cosa succederebbe se gli aggressori, chiunque essi siano, riuscissero a ottenere un ordigno nucleare in Russia, dove si ritiene che alcuni tipi di arma non vengano sorvegliati con cura. Mettono l'ordigno in un container e assumono criminali organizzati, magari mafiosi, per imbarcarlo su una nave volandiera a vapore. La nave scarica poi il container al porto di Dillingham, insieme a documenti falsi per spedirlo a Seattle. Il container viene poi caricato su una chiatta.

"'Dieci giorni dopo', il Capo della Polizia continua, 'la chiatta entra nel porto di Seattle'.

"Thompson fa una pausa a effetto.

"'Buuuuuum', dice, facendo con le mani il gesto di un fiore che sboccia".

Il primo problema di questa trama da film è che è semplicemente ridicola. Ma il secondo problema, e forse dovrete rileggere i particolari della storia per notarlo, è che quelle 80 telecamere non faranno nulla per fermare questo attacco immaginario.

Siamo tutti consumatori di sicurezza. Spendiamo denaro e ci aspettiamo una certa sicurezza in cambio. Questa spesa è stata un inutile spreco, e come contribuente americano sono piuttosto indispettito da questo bell'affare.

<<http://www.latimes.com/news/nationworld/nation/la-na-secure28mar28,0,2758659,full.story>> oppure <<http://tinyurl.com/ocfan>>

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

Le ristampe di Crypto-Gram

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

Attenuare il problema del furto d'identità:
<<http://www.schneier.com/crypto-gram-0504.html#2>>
<<http://www.cryptogram.it/cryptogramPdf/Aprile2005.pdf>> (traduzione)

Boicottare l'Elezione Papale:

<http://www.schneier.com/crypto-gram-0504.html#8>
<http://www.cryptogram.it/cryptogramPdf/Aprile2005.pdf> (traduzione)

Documenti d'identità nazionali:

<http://www.schneier.com/crypto-gram-0404.html#1>
<http://www.cryptogram.it/cryptogramPdf/Aprile2004.pdf> (traduzione)

Vincere illegalmente alle elezioni:

<http://www.schneier.com/crypto-gram-0404.html#4>
<http://www.cryptogram.it/cryptogramPdf/Aprile2004.pdf> (traduzione)

Attacco automatizzato di tipo Denial-of-Service sfruttando le Poste USA:

<http://www.schneier.com/crypto-gram-0304.html#1>
<http://www.cryptogram.it/aprile03.htm#a1> (traduzione)

La precisione del database NCIC (National Crime Information Center)

<http://www.schneier.com/crypto-gram-0304.html#7>
<http://www.cryptogram.it/aprile03.htm#a7> (traduzione)

Come pensare in merito alla sicurezza:

<http://www.schneier.com/crypto-gram-0204.html#1>
<http://www.cryptogram.it/aprile02.htm#a1> (traduzione)

1024 bit sono sufficienti?

<http://www.schneier.com/crypto-gram-0204.html#3>
<http://www.cryptogram.it/aprile02.htm#a3> (traduzione)

Responsabilità e sicurezza:

<http://www.schneier.com/crypto-gram-0204.html#6>
<http://www.cryptogram.it/aprile02.htm#a6> (traduzione)

I vantaggi naturali della difesa: che cosa può insegnare la storia militare alla sicurezza delle reti, prima parte:

<http://www.schneier.com/crypto-gram-0104.html#1>

Lo Uniform Computer Information Transactions Act (UCITA):

<http://www.schneier.com/crypto-gram-0004.html#ucita>

Crittografia: l'importanza di non essere diversi:

<http://www.schneier.com/crypto-gram-9904.html#different>

Minacce ai danni delle smart card:

<http://www.schneier.com/crypto-gram-9904.html#smartcards>

Attaccare i certificati con virus informatici:

<http://www.schneier.com/crypto-gram-9904.html#certificates>

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

Crittografia per VOIP

Esistono fondamentalmente quattro modi per intercettare una telefonata.

1) È possibile mettersi in ascolto da un altro apparecchio della stessa linea, da un altro interno. Questo è il metodo preferito da fratelli e sorelle in tutto il mondo. Avendo l'accesso giusto, è anche il più facile. Non funziona con i telefoni cellulari, ma i cordless sono vulnerabili a una variante di questo attacco: un ricevitore radio impostato sulla frequenza giusta può servire allo scopo.

2) È possibile collegare al cavo telefonico un qualche dispositivo di intercettazione con un paio di pinzette a coccodrillo. Ci vuole un po' di esperienza, ma si può effettuare questa operazione in qualsiasi punto della linea telefonica, anche al di fuori di un'abitazione. Questo metodo è stato il più utilizzato dalla polizia per intercettare le telefonate di un privato. Oggi probabilmente è più usato dai criminali. Neanche questo metodo funziona con i cellulari.

3) È possibile mettersi in ascolto alla centralina telefonica. Le moderne attrezzature telefoniche includono la possibilità di mettersi in ascolto in questo modo. Al momento è il sistema preferito dalla polizia. Funziona sia con la telefonia fissa sia con la telefonia mobile. È necessario l'accesso corretto, ma se si è in grado di ottenerlo, questa è forse la modalità più comoda per intercettare le chiamate di una persona.

4) È possibile intercettare le linee telefoniche primarie, mettersi in ascolto sui collegamenti telefonici via microonde o via satellite, ecc. Con questo sistema è difficile ascoltare un individuo in particolare, ma è semplice intercettare un intero blocco di chiamate. Questo è il tipo di sorveglianza costosa che organizzazioni come la National Security Agency svolgono al meglio. È risaputo che si sono servite perfino di sottomarini per intercettare le linee telefoniche subacquee.

Questo è in pratica il modello di minaccia per le telefonate tradizionali. E quando la maggior parte delle persone pensa alla telefonia IP (VOIP, ossia Voice Over Internet Protocol), probabilmente è il modello che ha in mente.

Purtroppo le chiamate che si originano dal proprio computer sono radicalmente differenti da quelle originate dal proprio telefono. Il modello di minaccia per la telefonia via Internet è molto più simile a quello dei computer collegati in rete mediante IP che non a quello della telefonia tradizionale.

Già conosciamo il modello di minaccia per l'IP. I pacchetti di dati possono essere intercettati _in qualsiasi punto_ del tracciato della trasmissione. Possono essere intercettati nella rete aziendale, dal provider di servizi Internet e lungo il backbone. Possono essere intercettati dagli individui o dalle organizzazioni che possiedono quei computer, e da chiunque sia riuscito a penetrare con successo in quei computer. Possono essere raccolti da hacker ficcanaso, da criminali, da concorrenti e da governi.

È paragonabile alla minaccia 3) vista prima, ma con un ambito notevolmente esteso.

La mia preoccupazione più grande sono gli attacchi criminali. Abbiamo già visto come negli ultimi anni i criminali si siano fatti sempre più scaltri nel rubare informazioni finanziarie e dati personali. Posso immaginarli intercettare avvocati e procuratori, a caccia di informazioni per ricattare le persone. O intercettare banchieri, a caccia di informazioni con le quali effettuare acquisti di titoli e azioni. Posso immaginarli rubare informazioni finanziarie, intercettare telefonate, commettere furti di identità. Sul lato degli affari, posso immaginarli fare spionaggio industriale e rubare segreti commerciali. Insomma, posso immaginarli compiere ogni genere di cosa che non avrebbero potuto fare con le linee telefoniche tradizionali.

Ecco perché la crittografia per VOIP è così importante. Le chiamate VOIP sono esposte a una varietà di minacce che non colpiscono le chiamate telefoniche tradizionali. La crittografia è una delle tecnologie di

sicurezza essenziali per i dati informatici, e ha un lungo cammino da percorrere per proteggere il VOIP.

L'ultima volta che si è parlato di questo genere di cose, il governo statunitense ha cercato di venderci qualcosa chiamato "key escrow". Fondamentalmente, al governo piace l'idea che tutti utilizzino la crittografia, purché il governo abbia una copia della chiave. Questa è un'idea incredibilmente poco sicura per tutta una serie di motivi, che si possono riassumere in questo modo: quando si mette a disposizione una modalità di accesso in un sistema di sicurezza, se ne indebolisce enormemente la sicurezza intrinseca.

Un caso accaduto di recente in Grecia lo ha dimostrato chiaramente: dei criminali hanno utilizzato un meccanismo di intercettazione per telefonia cellulare già predisposto e ideato affinché la polizia potesse effettuare intercettazioni telefoniche. Se il sistema di chiamate fosse stato progettato per essere sicuro prima di ogni altra cosa, non ci sarebbe stata una backdoor sfruttabile dai criminali.

Per fortuna esistono molti prodotti di crittografia per VOIP. Skype possiede una crittografia incorporata. Phil Zimmermann sta rilasciando Zfone, un prodotto open source facile da usare. Vi è persino una VOIP Security Alliance.

La crittografia per la telefonia IP è importante, ma non è una panacea. Fondamentalmente si occupa delle minacce dalla 2) alla 4) elencate all'inizio, ma non della 1). Purtroppo si tratta della minaccia più seria: l'intercettazione agli endpoint. Nessun tipo di crittografia per telefonia IP può impedire a un trojan o a un worm sul vostro computer (o a un hacker che è riuscito ad avere accesso alla vostra macchina) di intercettare le vostre chiamate; come analogamente nessuna crittografia SSL o e-mail può impedire a un trojan sul vostro computer di intercettare o modificare i vostri dati.

Pertanto, come sempre, tutto si riduce a questo: occorrono computer sicuri e sistemi operativi sicuri ancor prima di un sistema di trasmissione sicuro.

Perché il key escrow è una pessima idea:
<<http://www.schneier.com/paper-key-escrow.html>>

L'intercettazione avvenuta in Grecia:
<http://www.schneier.com/blog/archives/2006/02/phone_tapping_i.html>

Zfone:
<<http://www.philzimmermann.com/EN/zfone/index.html>>
<<http://www.wired.com/news/technology/0,70524-0.html>>

VOIP Security Alliance:
<<http://www.voipsa.org/>>

Questo articolo è originariamente apparso su Wired.com.
<<http://www.wired.com/news/columns/1,70591-0.html>>

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

Sicurezza mediante richieste formali

Da TechDirt: "La scorsa estate si è diffusa la notizia sorprendente secondo cui vi è stata una fuga di segreti nucleari giapponesi, dopo che un fornitore ha avuto il permesso di collegare il proprio computer,

infettato da un virus, alla rete di una centrale nucleare. Sul proprio portatile il fornitore aveva anche attiva un'applicazione di condivisione file per reti peer-to-peer, e i segreti nucleari sono stati subito a disposizione di ragazzini che stavano solo cercando di scaricarsi l'ultimo singolo di successo. Ci sono voluti solo nove mesi circa prima che il governo elaborasse la propria proposta per evitare fughe di notizie di questo genere in futuro: richiedere formalmente a tutti i cittadini giapponesi di non utilizzare sistemi di condivisione dei file, così la prossima volta che accadrà una cosa del genere, nessuno si troverà in rete a scaricare quei documenti".

Anche se tale richiesta formale funzionerà, risolverà il problema sbagliato. Che tristezza.

L'articolo:

<http://techdirt.com/articles/20060316/0052241.shtml>

L'articolo originale:

<http://www.techdirt.com/articles/20050623/0251255.shtml>

La proposta del governo:

<http://mdn.mainichi-msn.co.jp/national/news/20060315p2a00m0na017000c.html> oppure <http://tinyurl.com/pejx2>

Un altro articolo:

<http://www.latimes.com/news/nationworld/world/la-fg-computer21mar21,0,5159274.story> oppure <http://tinyurl.com/fmvlb>

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

Il Privacy and Integrity Report del Dipartimento per la Sicurezza Nazionale

Lo scorso anno, il Dipartimento per la Sicurezza Nazionale è finalmente riuscito a nominare la propria assemblea consultiva sulla Privacy e l'Integrità dei Dati (Data Privacy and Integrity Advisory Committee). Era costituito soprattutto da figure interne all'industria invece che da individui con una reale esperienza in merito alla privacy (Lance Hoffman della George Washington University era l'eccezione più notevole).

E ora siamo in possesso di ciò che ha prodotto quell'assemblea. Il 7 marzo hanno pubblicato il loro Framework per l'Analisi della Privacy di Programmi, Tecnologie e Applicazioni (Framework for Privacy Analysis of Programs, Technologies, and Applications).

È sorprendentemente buono.

Mi piace che sia organizzato come una serie di domande a cui un program manager deve rispondere: sulla base legale del programma, la sua efficacia contro la minaccia, e i suoi effetti sulla privacy. Mi fa soprattutto piacere che le domande presenti alle pagine 3 e 4 siano molto simili ai "cinque passi" da me trattati in "Beyond Fear". Sono elettrizzato dal fatto che il documento affronti la questione in termini di compromessi e bilanciamenti; l'ultima domanda chiede: "Il programma deve procedere? I benefici del programma [...] giustificano i costi per gli interessi della privacy [...]?"

Credo che questo sia un ottimo punto di partenza per qualsiasi tecnologia o programma che tenga in considerazione sicurezza e privacy. E spero che il Dipartimento per la Sicurezza Nazionale segua davvero i

consigli presenti in questo rapporto.

L'Assemblea:

http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0512.xml

http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0598.xml

Il Framework per l'Analisi della Privacy di Programmi, Tecnologie e Applicazioni:

http://www.privacilla.org/releases/DHS_Privacy_Framework.pdf

I miei "cinque passi":

<http://www.schneier.com/crypto-gram-0204.html#1>

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

News

È ovvio che i chip RFID possono trasmettere virus, in fondo sono piccoli computer.

<http://arstechnica.com/news.ars/post/20060315-6386.html>

Ritengo che il vettore di attacco sia interessante: un RFID trojan attacca il database centrale invece di attaccare direttamente altri chip RFID. Metaforicamente è assai simile ai virus biologici, perché richiede che venga sovvertito l'ospite più potente, e non c'è modo che un tag infettato possa propagarlo direttamente a un altro tag. La notizia, tuttavia, è trattata con toni un po' troppo sensazionalistici.

<http://www.computerworld.com/mobiletopics/mobile/story/0,10801,109560,00.html> oppure <http://tinyurl.com/mwz88>

I cinema vogliono effettuare il jamming dei telefoni cellulari.

<http://www.mobiletracker.net/archives/2006/03/15/movie-theater-jamming>

<http://www.csmonitor.com/2006/0324/p11s01-almo.html>

Massiccia sorveglianza nel mondo virtuale di un noto gioco online.

http://terranova.blogs.com/terra_nova/2006/03/confessions_of_.html

Yossi Oren e Adi Shamir hanno scritto uno studio che descrive un power attack contro i tag RFID. Si tratta di un ottimo lavoro da parte di Oren e Shamir. Dall'abstract: "Power analysis dei Tag RFID: comparato ai normali attacchi power analysis, questo attacco è unico nel suo genere in quanto non richiede il contatto fisico con il dispositivo sotto attacco. Mentre l'attacco specifico qui descritto richiede che l'aggressore trasmetta effettivamente dei dati al tag sotto attacco, la parte power analysis stessa ha soltanto bisogno di un'antenna ricevente. Ciò significa che una variante di tale attacco può essere progettata in modo che l'aggressore rimanga totalmente passivo durante l'acquisizione dei dati, rendendo l'attacco molto difficile da rilevare". La mia previsione sulla risposta da parte dell'industria: minimizzare i risultati dello studio e far finta che non sia un problema.

<http://www.wisdom.weizmann.ac.il/%7Eyossio/rfid/>

La terza Nigerian E-mail Conference. Divertente.

<http://j-walk.com/other/conf/index.htm>

Il direttore della Qantas è stato fermato dalla sicurezza aeroportuale. Era in possesso di eliografie di aeroplani. Ah, e poi si trattava di una donna, il che rendeva immediatamente sospetta la sua storia.

<http://www.aero-news.net/Community/DiscussTopic.cfm?TopicID=2648&Refresh=1>

Articolo davvero ottimo di un reporter che ha parlato in maniera esauriente degli ordigni esplosivi improvvisati in Iraq:

<http://www.defensetech.org/archives/002238.html>

Esistono delle banconote da 300, 600 e 1000 euro dichiaratamente false, realizzate in Germania come trovata pubblicitaria. Vengono fatte passare come vere:

http://www.ananova.com/news/story/sm_1760580.html

Ecco il motivo per cui la sicurezza è così difficile: le persone.

Un articolo veramente interessante a firma Robert X. Cringely sulla mancanza di finanziamenti federali per le tecnologie di sicurezza. Ritengo che la sua analisi centri perfettamente il punto.

<http://www.pbs.org/cringely/pulpit/pulpit20060309.html>

Frode bancaria in Australia: mi piacerebbe che questo articolo contenesse maggiori dettagli sul reato. Sostanzialmente, un gruppo di malviventi ha utilizzato un'omissione di autenticazione nelle trasmissioni via fax per sottrarre (senza successo, come si è visto) 150 milioni di dollari australiani.

<http://www.smh.com.au/articles/2006/03/17/1142582520870.html>

Raro impeto di buonsenso in termini di sicurezza a Londra. Stanno scartando lo screening dei passeggeri nella rete metropolitana.

<http://www.kablenet.com/kd.nsf/Frontpage/85C58F53F411521180257132005EF49F?OpenDocument> oppure <http://tinyurl.com/nrmpr>

Chi ha bisogno dei terroristi? Possiamo provocare terrore per conto nostro.

<http://www.postgazette.com/pg/06081/674773.stm>

La vicenda parla di una reazione oltremodo eccessiva in ambito di sicurezza perché un dipendente in un edificio del centro stava usando una pistola ad aria compressa per spaventare i piccioni.

Ennesima minaccia da trama cinematografica nella variante "Terroristi con armi nucleari". Pare che questo scrittore del New Scientist stia cercando di scrivere un romanzo.

http://archinect.com/news/article.php?id=35501_0_24_15_M

Enigma? Non so che cosa sia questo, ma di sicuro assomiglia davvero a un Enigma. Ed è bellissimo.

<http://www.tatjavanvark.nl/tvv1/pht10.html>

Una coppia, suppongo convivente, di fidanzati prossimi al matrimonio condivideva un computer. Lui utilizzava Firefox per visitare una serie di siti per incontri casuali, avendo l'accortezza di evitare che il browser registrasse la sua password. Ma Firefox ha conservato i nomi dei siti per i quali non doveva registrare la password. Lei ha trovato per caso l'elenco di questi siti. I dettagli vengono lasciati all'immaginazione, in ogni caso i due si sono lasciati.

https://bugzilla.mozilla.org/show_bug.cgi?id=330884

Il bug report più interessante che mi sia mai capitato di leggere.

Creative Home Engineering è un'azienda che può realizzare porte nascoste e passaggi segreti per la vostra casa. "Spostate uno dei vostri libri preferiti da una mensola della libreria e osservate mentre una sezione della stessa si sposta verso l'interno per rivelare un passaggio segreto. Girate un candeliere e il vostro caminetto ruota e vi permette di accedere a una stanza nascosta". Chi se ne importa delle caratteristiche di sicurezza? Ne voglio uno.

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

Crittografia mediante quasar:

<http://www.theinquirer.net/?article=30553>
http://www.schneier.com/blog/archives/2006/03/quasar_encrypti.html

È stato catturato un hacker al servizio di al Qaeda, chiamato Irhabi 007. Assumendo che le autorità britanniche dicano il vero, questo individuo si trattava decisamente di un terrorista. E si serviva di Internet, sia come mezzo di comunicazione, sia per penetrare all'interno di altre reti. Ma questo non lo rende un terrorista cibernetico.

<http://www.washingtonpost.com/wp-dyn/content/article/2006/03/25/AR2006032500020.html>

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

<http://it.slashdot.org/article.pl?sid=06/03/26/0530206>

La polizia si è servita di profili su MySpace per identificare sei sospettati in un furto con stupro.

<http://www.cnn.com/2006/US/03/25/my.space.ap/index.html>

Armi camaleonte: non è possibile rilevarle perché appaiono normali.

<http://www.defensetech.org/archives/002265.html>

Un'analisi economica dello screening di sicurezza degli aeroporti. Gli autori si servono della teoria del gioco per investigare la linea di condotta ottimale per lo screening, in uno scenario in cui sono presenti diversi gruppi sociali (separati da criminali, razza, religione, ecc.) con preferenze diverse per quanto riguarda il crimine e/o il terrorismo.

<http://www.econ.upenn.edu/~persico/research/Papers/airportaeall.pdf>

I "cubicle farm" (grandi uffici suddivisi in cubicoli) sono a rischio terrorismo.

Il servizio di sicurezza britannico MI5 sta avvertendo le varie aziende leader del mercato riguardo a una possibile inefficace progettazione dei loro uffici contro ordigni terroristici. Il tipico ufficio moderno è costituito da ampie stanze prive di pareti interne, il che pone maggiormente a rischio gli impiegati in caso di bombe.

<http://news.scotsman.com/index.cfm?id=419082006>

Non so se questo "Internet Hash Project" sia un pesce d'Aprile, ma è ugualmente divertente.

<http://www.nethash.org/>

Lo scorso mese il Government Accounting Office ha rilasciato tre nuovi rapporti sulla sicurezza nazionale.

"Cargo Container Inspections: Preliminary Observations on the Status of Efforts to Improve the Automated Targeting System" [Ispezioni dei container di carico: Osservazioni Preliminari sullo Stato dei Lavori per migliorare il Sistema di Tracciamento Automatico].

<http://www.gao.gov/cgi-bin/getrpt?GAO-06-591T>

Punti salienti: <http://www.gao.gov/highlights/d06591thigh.pdf>

"Homeland Security: The Status of Strategic Planning in the National Capital Region" [Sicurezza Nazionale: lo Stato della Pianificazione Strategica nella Regione Capitale Nazionale]

<http://www.gao.gov/cgi-bin/getrpt?GAO-06-559T>

Punti salienti: <http://www.gao.gov/highlights/d06559thigh.pdf>

"Homeland Security: Progress Continues, but Challenges Remain on Department's Management of Information Technology" [Sicurezza Nazionale: Continuano i progressi, ma rimangono le difficoltà sulla gestione dell'Information Technology da parte del Dipartimento].

<http://www.gao.gov/cgi-bin/getrpt?GAO-06-598T>

Punti salienti: <http://www.gao.gov/highlights/d06598thigh.pdf>

È un'idea davvero intelligente: catenacci e chiavistelli che si chiudono e si aprono in risposta a comandi remoti impartiti via computer. Ma il commento sulla sicurezza è buffo: "Ma ogni cosa viene serrata e

assicurata da codici, e i segnali radio vengono codificati, pertanto il tutto è assolutamente protetto dagli hacker". È ovvio che questo tizio non sa nulla di sicurezza informatica.

<http://www.chicagotribune.com/business/chi-0603300225mar30,1,7805363.story> oppure <http://tinyurl.com/rtoxc>
<http://it.slashdot.org/article.pl?sid=06/04/03/0624225>

Studio interessante sul phishing e perché funziona.

http://www.deas.harvard.edu/~rachna/papers/why_phishing_works.pdf

Investigatori sotto copertura sono stati in grado di introdurre illegalmente materiali radioattivi negli Stati Uniti. Ai checkpoint di frontiera sono scattati gli allarmi, ma i "contrabbandieri" erano in possesso di licenze di importazione falsificate della Nuclear Regulatory Commission, basate su un'immagine di un documento reale trovata in Internet. Purtroppo gli agenti di frontiera non avevano alcun mezzo per confermare la validità delle licenze d'importazione. Ho trattato questo problema in passato, e ritengo che sia un problema che andrà peggiorando in futuro. I sistemi di verifica sono spesso l'anello più debole dell'autenticazione. Migliorare i token di autenticazione non garantirà una sicurezza migliore, a meno che i sistemi di verifica non migliorino di pari passo.

http://www-tech.mit.edu/V125/N1/long4_1.lw.html

http://www.schneier.com/blog/archives/2006/01/forged_credenti.html

Applicazioni di sicurezza dell'inversione del tempo acustica.

Semplicemente non sono in possesso delle conoscenze necessarie per darne una valutazione.

<http://www.physorg.com/news12093.html>

I legislatori dell'Iowa stanno proponendo una tessera "Non sono il Criminale che state cercando", per le vittime di furti d'identità. Penso che sia un'ottima idea, e mi ricorda qualcosa che ho trattato in "Beyond Fear": "A Singapore alcuni nomi sono talmente comuni che la polizia emette documenti che attestano che 'lui non è il tizio che stiamo cercando', i quali esonerano le persone innocenti che portano lo stesso nome di criminali ricercati". Non è un progetto perfetto, e naturalmente queste tessere verranno falsificate; tutti i documenti vengono falsificati. Ma anche se non è perfetta, rimane sempre una buona idea.

http://news.com.com/Iowa+proposes+ID+theft+passport/2100-7348_3-6052308

Ottime informazioni da parte dell'EPIC sulla sicurezza dei dati fiscali nell'IRS.

<http://www.epic.org/privacy/surveillance/spotlight/0306/>

Un uomo nel Regno Unito è stato arrestato per aver canticchiato una canzone dei Clash. Lo ha denunciato il tassista.

http://today.reuters.co.uk/news/newsArticle.aspx?type=entertainmentNews&storyID=2006-04-05T134826Z_01_L05785309_RTRUKOC_0_UK-CLASH.xml oppure

<http://tinyurl.com/e6nr6>

<http://news.bbc.co.uk/1/hi/england/4879918.stm>

Mi trovavo a New York all'inizio del mese, e ho visto un cartello all'ingresso del Midtown Tunnel che diceva: "See something? Say something" [Visto qualcosa? Riferitelo]. Il problema di una nazione di spie amatoriali è che si finisce con l'avere questi risultati. "So che è un terrorista perché si veste in modo strano e ha sempre dei cavetti bianchi che penzolano dalle tasche". "Parlano tutti una strana lingua e la loro cucina puzza terribilmente". Le spie amatoriali non fanno altro che spionaggio amatoriale. Se tutti seguono l'esempio, la polizia sarà sommersa dai falsi allarmi.

Tutti avete sentito parlare della "No-Fly List". Sapevate che esiste anche una "No-Buy List"?

KittenAuth funziona con le immagini. Il sistema mostra nove figure di animaletti simpatici, e la persona si autentica facendo clic sui tre gattini. Un computer che effettua la scelta in modo casuale ha una probabilità su 84 di indovinare.

Ovviamente è possibile aumentare la sicurezza aggiungendo più immagini o richiedendo alla persona di scegliere più immagini. Un'altra preoccupazione, che non vedo trattata, è che il computer possa effettuare un attacco di forza bruta ai danni di un database statico. Se vi è soltanto un ridotto numero fisso di gattini veri e propri, il computer potrebbe essere istruito da una persona a riconoscerli come gattini. In seguito il computer saprebbe che ogni volta in cui viene presentata quell'immagine si tratta di un gattino.

Però rimane un'idea interessante, che merita ulteriori ricerche.

KittenAuth:

<http://www.thepcspy.com/articles/security/the_cutest_humantest_kittenauth> oppure <<http://tinyurl.com/o2585>>

I CAPTCHA:

<<http://en.wikipedia.org/wiki/Captcha>>

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

I rischi di tipo terroristico di Google Earth

A volte mi meraviglio di certi "esperti di sicurezza". Eccone uno che pensa che Google Earth sia un rischio di tipo terroristico perché permette alle persone di conoscere le coordinate GPS degli stadi calcistici.

In sostanza, Klaus Dieter Matschke è preoccupato perché Google Earth fornisce la posizione degli edifici nel raggio di 20 metri, mentre in precedenza le coordinate avevano un intervallo di errore di un chilometro. È preoccupato che tali informazioni possano offrire ai terroristi le coordinate esatte dei bersagli di possibili attacchi missilistici.

Non ho la più pallida idea del perché qualcuno possa stampare tali stupidaggini. Chiunque può assistere a una partita di calcio con un ricevitore GPS in tasca e ottenere le coordinate con una precisione di un metro. O può comprarsi una mappa.

Google Earth non è il problema; il problema è la disponibilità di missili a corto raggio sul mercato nero.

<<http://www.heise.de/newsticker/meldung/71784>>

Post di un blog in inglese sull'argomento:

<<http://www.ministryofpropaganda.co.uk/2006propaganda/20060409-googleearth.shtml>> oppure <<http://tinyurl.com/lpay3>>

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

Un nuovo tipo di serratura

L'azienda israeliana E-Lock ha prodotto un nuovo tipo di serratura per

porte. Risponde a stimoli sonori. Invece di una chiave, portate con voi un piccolo dispositivo che emette una rapida sequenza di suoni che "bussano" alla porta. Basta che entri in contatto con la porta e questa si apre; non c'è un buco della serratura. Il dispositivo, chiamato "KnockKey", ha un tastierino che può essere programmato in modo da richiedere un PIN prima di mettersi in funzione, per una sicurezza ancora maggiore.

Idea astuta, ma vi è la solita iperbole sulla sicurezza: "Dato che non esiste un buco della serratura o un punto di contatto sulla porta, questo meccanismo unico nel suo genere offre un livello di sicurezza decisamente più alto rispetto alle tecnologie esistenti".

Più esatto sarebbe affermare che le vulnerabilità di sicurezza sono diverse rispetto alle tecnologie esistenti. Sappiamo molto delle vulnerabilità delle serrature convenzionali, ma sappiamo davvero poco della sicurezza di questo sistema. Ma non si confonda questa mancanza di conoscenza con una maggiore sicurezza.

<http://www.elock.co.il/tech-english.asp>

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

Le News di Counterpane

Bruce Schneier interverrà al Symposium on Business Information Security a Minneapolis il 21 aprile:
https://www.minneapolis.edu/sobis/files_pdf/SoBIS2006-Flyer.pdf

Bruce Schneier interverrà al CardTech/SecureTech a San Francisco il 3 maggio.
<http://www.ctst.com/conferences/CTST06/>

Bruce Schneier e Toby Weir-Jones sono intervenuti all'InfoWorld Webcast intitolato "Managed Compliance Reporting: Best Practices to Streamline Device Management & Demonstrate Compliance". È disponibile una replica della trasmissione.
<http://w.on24.com/r.htm?e=21082&s=1&k=9A69DBFE212400FB9B547D40A596F856&partnerref=CIS1> oppure <http://tinyurl.com/lzxab>

Counterpane sta offrendo posti di lavoro. Fra le varie figure stiamo cercando un Database e System Analyst, un Senior Java Software Engineer e un SOC intelligence officer.
<http://www.counterpane.com/jobs.html>

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

Aggirare il copyright mediante XOR

Monolith è un programma open source che può fare lo XOR di due file per creare un terzo file e, naturalmente, può fare lo XOR di quel terzo file con uno dei due originali per ricreare l'altro file originale.

Il sito Web si chiede le conseguenze di tutto questo a livello di copyright: "Le cose si fanno interessanti quando si applica Monolith a file protetti da copyright. Per esempio, incrociando due file protetti da copyright si produrrà un terzo file completamente nuovo che, nella maggior parte dei casi, non conterrà alcuna informazione dei due file originali. In altre parole, il file Mono risultante non è di proprietà

di chi detiene il copyright dei file originali (se fosse proprietà di qualcuno, sarebbe della persona che ha incrociato i due file). Dato che il file Mono può essere combinato con uno dei due file originali (e protetti da copyright) per ricostruire l'altro file protetto da copyright, questa mancanza di proprietà del file Mono può sembrare incredibile".

Il sito Web, poi, postula questo procedimento come un meccanismo per aggirare la legge sul copyright:

"Che significa tutto questo? Significa che i file Mono possono essere liberamente distribuiti.

"E quindi? I file Mono sono inutili senza i loro file Base corrispondenti, giusto? E i file Base sono protetti da copyright, per cui non possono essere liberamente distribuiti, giusto? Ma questa idea può prendere una piega inaspettata. Che succede quando si utilizzano file Base liberamente distribuibili? Per esempio, si potrebbe usare un file Base che è di dominio pubblico oppure che possiede una licenza per la libera distribuzione. Adesso stiamo facendo progressi.

"Nessuna delle summenzionate proprietà dei file Mono cambia quando si utilizzano file Base liberamente distribuibili, dato che valgono le stesse argomentazioni. I file Mono non sono di proprietà delle stesse entità che possiedono i diritti di copyright dei file Element originali corrispondenti. Ora possiamo liberamente distribuire file Mono e file Base.

"Interessante? Non proprio. Ma potrebbe essere interessante quel che si può fare con questi file nella privacy della propria dimora, a seconda dei gusti. Per esempio, si possono usare i file Mono e i file Base per ricostruire i file Element".

Molto astuto, ma non può reggere di fronte a un tribunale. In generale, il cercare il pelo nell'uovo dei dettagli tecnici non è un sistema efficace per aggirare la legge. La mia ipotesi è che chiunque distribuisca quel terzo file (lo chiamano "file Mono") unitamente alle istruzioni per ricostruire il file protetto da copyright è destinato a essere incriminato per violazione del copyright.

Il metodo corretto per risolvere il problema è attraverso la legge, non attraverso la tecnologia.

[<http://monolith.sourceforge.net/>](http://monolith.sourceforge.net/)

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

iJacking

Si chiama iJacking: rubare computer portatili dalle mani dei loro proprietari e fuggire via. Pare vi sia un'ondata di questo genere di reato negli Internet café di San Francisco.

Il perché avvengano questi furti è scontato: i portatili sono oggetti di valore, facili da rubare e facili da rivendere. Se vogliamo "risolvere" il problema dobbiamo modificare almeno una di tali caratteristiche. Alcuni Internet café offrono cavi di sicurezza per gli avventori, così che possano assicurare il loro portatile e renderlo più difficile da rubare. Ma questo non risolve il problema, e spingerà i rapinatori a seguire le loro vittime una volta uscite dall'Internet café. I computer portatili perderanno di valore col tempo, ma neanche questa è una buona

soluzione. L'unica soluzione rimasta è quella di renderli più difficili da rivendere.

Non si tratta di un problema semplice. Vi sono diverse aziende che producono soluzioni per aiutare le persone a recuperare portatili rubati. Vi sono programmi che "chiamano casa" se il computer viene rubato. Vi sono programmi che nascondono un numero seriale in qualche punto dell'hard disk. Vi sono etichette non asportabili che gli utenti possono attaccare sui propri computer e sulle quali riportare informazioni di identità. Ma fino a quando queste soluzioni non saranno più diffuse, i furti continueranno.

Mi ricorda il problema dei furti di biciclette.

http://www.sfbg.com/40/25/news_ijacked.html

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

Screening di sicurezza per gli elicotteri di New York

Vi è un elicottero navetta che unisce Lower Manhattan e il Kennedy Airport. È in sostanza un'opzione di lusso: per 139 dollari si può evitare di guidare fino all'aeroporto. Ma naturalmente è necessaria la presenza di screener di sicurezza per i passeggeri, e ciò è fonte di preoccupazione:

"A seguito della richiesta della direzione della U.S. Helicopter, la Transportation Security Administration ha istituito un checkpoint dotato di macchine a raggi X e attrezzature per il rilevamento di ordigni esplosivi, per effettuare lo screening dei passeggeri e del loro bagaglio all'interno dell'eliporto.

"L'agenzia di sicurezza quest'anno sta spendendo 560.000 dollari per far funzionare il checkpoint con una squadra di otto screener e sta considerando l'aggiunta di un checkpoint all'eliporto all'east end di 34th Street. Il coinvolgimento dell'agenzia ha attratto le critiche da parte di alcuni funzionari eletti.

"Il nocciolo del problema qui è che non c'è un numero sufficiente di screener", ha dichiarato il Senatore Charles E. Schumer, democratico di New York. "Il problema è che per soddisfare un mercato di lusso stiamo sottraendo screener che sono necessari agli aeroporti, e questo alle spese del governo".

Questo non è un problema di sicurezza, è un problema di economia. Ed è un'ottima dimostrazione del concetto di "esternalità". Un'esternalità è l'effetto di una decisione che non viene sostenuto da chi ha preso quella decisione. In questo esempio, la U.S. Helicopter ha preso la decisione commerciale di offrire tale servizio a un certo prezzo. E i clienti decideranno se il servizio valga o meno i soldi spesi. Ma il costo non è limitato a quei 139 dollari. Il costo di quel checkpoint è un'esternalità sia per U.S. Helicopter sia per i suoi clienti, perché i 560.000 dollari investiti nel checkpoint di sicurezza vengono pagati dai contribuenti. E in realtà sono proprio i contribuenti a sovvenzionare il costo reale della corsa in elicottero.

L'unico modo per risolvere la questione, da parte del governo, è quello di far pagare ai passeggeri delle linee aeree il costo dello screening di sicurezza. Non dovrebbe essere un aumento considerevole del singolo biglietto, diciamo 15 dollari. E sarebbe inferiore negli aeroporti più grandi, perché l'economia di scala è molto maggiore.

L'articolo sostiene persino che i clienti sarebbero lieti di pagare i 15 dollari extra grazie a un'altra esternalità: le persone che decidono di fare o meno la corsa in elicottero non sono le persone che in effetti pagano quel servizio.

"Bobby Weiss, un libero professionista operatore di borsa e broker immobiliare che ieri è stato il primo cliente pagante di U.S. Helicopter, ha dichiarato che avrebbe pagato 300 dollari per un viaggio andata e ritorno al Kennedy Airport, e che si aspetta che molti dirigenti d'azienda sarebbero disposti a fare altrettanto.

"Sono 300 dollari, e allora? Finisce nel conto spese", ha detto il signor Weiss, aggiungendo di non avere alcun rimorso in merito al dirottamento di fondi federali per agevolare chi vola ad alta quota. "Magari un tizio più ricco può risparmiarne un po' di tempo alle spese di un tizio più povero che passa un po' più di tempo in coda".

Quel che il signor Weiss sta dicendo è che i costi, sia il costo diretto sia quello del checkpoint di sicurezza, per lui sono un'esternalità, e quindi a lui non importa un granché. Appunto.

<http://www.nytimes.com/2006/02/06/nyregion/06chopper.html?ex=1296882000&en=1e835454a0fealc9&ei=5088&partner=rssnyt&emc=rss> oppure <http://tinyurl.com/lebvfb>

** **

Commenti dei lettori

Su questi argomenti vi sono centinaia di commenti nel mio blog, molti davvero interessanti. Cercate la vicenda sulla quale intendete dare la vostra opinione, e unitevi al dibattito.

<http://www.schneier.com/blog>

** **

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

I numeri arretrati sono disponibili all'indirizzo

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

Per iscriversi, cancellare l'iscrizione o cambiare il proprio indirizzo a cui recapitare la newsletter, visitate:

<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.

Crypto-Gram è una newsletter personale. Le opinioni qui espresse non sono necessariamente quelle di Counterpane Internet Security, Inc.

Copyright (c) 2006 by Bruce Schneier.