

Alla fine del mese, il post nel mio blog contava 782 commenti. Mi aspettavo molta partecipazione, ma una tale risposta mi ha lasciato sbalordito.

Osservando le varie trame terroristiche, pare che si possano far rientrare in diverse categorie generali. Una prima categoria riguarda gli attacchi contro l'infrastruttura degli Stati Uniti: la riserva di cibo, di acqua, l'infrastruttura energetica, il sistema telefonico, ecc. L'idea è quella di danneggiare il paese prendendo di mira uno dei sistemi fondamentali che lo sostengono.

Una seconda categoria prevede trame "ad alto costo": o prendono di mira bersagli pubblici e ben in vista (far saltare in aria il Super Bowl, la cerimonia degli Oscar, e così via), oppure prevedono componenti ad alta tecnologia: scorie nucleari, antrace, cloro in forma di gas, una petroliera a pieno carico, ecc. Spesso queste trame sono complesse e difficili da realizzare. È l'idea dell'11 settembre: un unico evento di enorme portata che va a colpire l'intero paese.

La terza categoria prevede ripetuti attacchi a bassa tecnologia. Molte persone hanno pensato a una versione del "cecchino di Washington" da realizzarsi con più squadre. I vari gruppi si sposterebbero pian piano attraverso il paese, per esempio un gruppo potrebbe attivarsi dopo l'arresto o l'eliminazione del gruppo precedente. Altre persone hanno suggerito una variante a questa trama: piccoli ordigni esplosivi disposti casualmente in zone pubbliche in tutto il paese.

(Vi è una quarta categoria: trame da film vere e proprie. Alcune proposte sono comiche, non realistiche, con premesse fantascientifiche, ecc. Non le considero nemmeno).

Le idee migliori fanno leva direttamente sulle pubbliche paure. Nel mio libro "Beyond Fear" ho delineato e trattato cinque diverse tendenze con cui le persone ingigantiscono i rischi, ovvero ritengono che qualcosa sia molto più pericoloso di quanto lo è realmente.

1. Le persone ingigantiscono rischi spettacolari ma rari e sminuiscono i rischi più comuni.
2. Le persone hanno difficoltà a calcolare i rischi legati a qualsiasi scenario che si discosta dalla loro situazione normale.
3. I rischi personificati vengono percepiti come più gravi di quelli anonimi.
4. Le persone sottovalutano i rischi che decidono di correre volontariamente e sopravvalutano i rischi legati a situazioni che non possono controllare.
5. Le persone sopravvalutano quei rischi che vengono continuamente discussi e che rimangono al centro dell'attenzione dell'opinione pubblica.

Le idee migliori per una trama terroristica fanno leva su una o più tendenze fra quelle elencate. Gli attacchi "ad alto costo" fanno leva sulla prima. Attacchi alle infrastrutture e attacchi a bassa tecnologia fanno leva sulla quarta. E ogni attacco cerca di far leva sulla quinta, specialmente gli attacchi ripetuti. Scommetto che il vincitore del mio concorso sarà il piano d'attacco che sfrutta il maggior numero delle tendenze sopra elencate per ottenere il miglior vantaggio possibile.

Ho anche ricevuto alcune email di persone che ritenevano di avere idee

troppo orribili per poter essere pubblicate e divulgate. Alcuni si rifiutavano di comunicarle persino a me. Altri messaggi email, invece, mi accusavano di aiutare i terroristi in questo modo, fornendo loro nuove idee.

Ma se vi è una cosa che questo concorso dimostra, è che vi sono decine di buone idee per piani terroristici. Chiunque è in grado di pensare a un sistema per provocare terrore. La parte difficile è realizzarlo.

Alcune delle trame proposte richiedono poca esperienza e attrezzatura. Venti uomini dotati di armi e automobili, una cosa del genere. Facendo scorrere le varie proposte uno si domanda perché non vi siano stati attacchi terroristici negli Stati Uniti dall'11 settembre 2001. Non credo alla "teoria della carta moschicida" secondo cui i terroristi sono tutti in Iraq invece che negli Stati Uniti. E malgrado l'inefficienza di tutta la sicurezza che abbiamo implementato dall'11 settembre in poi, sono certo che vi sono stati dei progressi a livello di intelligence e di investigazioni, progressi che hanno reso più difficile per i terroristi operare sia negli Stati Uniti che all'estero.

Ma soprattutto credo che gli attacchi terroristici siano molto più complessi da realizzare di quanto si pensi. Trovare reclute volontarie è molto più difficile di quanto pensiamo. Stesso dicasi per il coordinamento dei piani. E per l'esecuzione di quei piani. Il terrorismo è un fenomeno raro, e malgrado tutto quel che abbiamo sentito su come l'11 settembre abbia cambiato il mondo, il terrorismo continua a essere un fenomeno raro.

La scadenza del concorso era la fine di aprile, ma vi prego di continuare a inviare trame e complotti, se vi vengono delle idee. E vi prego di leggere le proposte altrui e commentarle: sono curioso di sapere quali siano, a vostro parere, gli scenari più interessanti, avvincenti, realistici o efficaci.

Sto continuando a leggere le varie proposte, e un vincitore sarà annunciato sul prossimo numero di Crypto-Gram.

Il concorso:

http://www.schneier.com/blog/archives/2006/04/announcing_movi.html

La teoria della carta moschicida:

http://en.wikipedia.org/wiki/Flypaper_theory_%28strategy%29

Anche il New York Times parla del concorso:

<http://www.nytimes.com/2006/04/23/movies/23peterson.html?ex=1303444800&en=c7ccc8d756fc98e7&ei=5090&partner=rssuserland&emc=rss>

oppure <http://tinyurl.com/qyh3b>

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

Chi possiede il vostro computer?

Quando la tecnologia è al servizio di chi la possiede, fa sentire liberi. Quando viene progettata per essere al servizio di altri, ignorando la volontà di chi la possiede, allora diventa oppressiva. Proprio adesso, nei vostri computer, è in atto una vera e propria battaglia, che vi vede opposti a worm e virus, trojan, spyware, update automatici e tecnologie per la gestione dei diritti digitali. È la battaglia per determinare chi possiede il vostro computer.

Ovviamente siete voi a possedere il computer. Lo avete acquistato. Avete

pagato per averlo. Ma quanto controllo avete realmente su ciò che accade nella vostra macchina? Tecnicamente potete anche aver acquistato l'hardware e il software, però vi ritrovate ad avere meno controllo su ciò che stanno facendo dietro le quinte.

Per usare un termine del gergo hacker, il vostro computer è "owned" (posseduto) da altri.

Tradizionalmente solo hacker malevoli cercavano di possedere i vostri calcolatori. Attraverso worm, virus, Trojan o altri mezzi, il loro tentativo era quello di installare sul vostro sistema un qualche tipo di programma per controllarlo da remoto. Poi avrebbero utilizzato i vostri computer per lo sniffing di password, per effettuare transazioni bancarie fraudolente, per inviare spam, intentare attacchi di phishing e così via. Secondo alcune stime si dice che il numero di computer che fanno parte di network "bot" controllate a distanza si aggiri fra le centinaia di migliaia e i milioni di unità. Tutte "owned".

Oggi le cose non sono così semplici. Vi sono svariati tipi di interessi in gioco per ottenere il controllo del vostro computer. Le aziende dei media vogliono controllare che cosa potete fare con la musica e i video che vi vendono. Vi sono compagnie che utilizzano il software come veicolo di raccolta di informazioni di marketing, per distribuire pubblicità o fare qualsiasi cosa venga richiesta dai loro proprietari. Vi sono aziende di software che cercano di fare soldi soddisfacendo non soltanto i propri clienti, ma anche altre compagnie con cui si alleano. Tutte queste compagnie vorrebbero possedere il vostro computer.

Alcuni esempi:

1. Software d'intrattenimento - Nell'ottobre 2005 si è saputo che Sony aveva distribuito un rootkit all'interno di parecchi CD musicali, ossia lo stesso genere di software che i cracker sfruttano per accedere e possedere i computer altrui. Questo rootkit si installava di nascosto quando il CD musicale veniva riprodotto sul computer. Il suo scopo era di evitare che le persone utilizzassero la musica in modalità non gradite a Sony. Si trattava quindi di un sistema DRM. Se lo stesso identico software fosse stato installato di nascosto da un hacker sarebbe stato un atto illecito. Ma Sony evidentemente credeva di avere motivi legittimi per voler "possedere" le macchine dei propri clienti.

2. Antivirus - Il vostro software antivirus avrebbe dovuto rilevare il rootkit di Sony, o almeno così vi aspettavate. Dopotutto è per questo che lo avete acquistato. Ma inizialmente i programmi di sicurezza venduti da Symantec e altri produttori non lo rilevavano, perché Sony aveva chiesto loro di non farlo. Avreste potuto pensare che il software da voi comprato stesse lavorando per voi, ma così non è stato.

3. Servizi Internet - Hotmail vi permette di mettere in black list certi indirizzi email, così che i messaggi da essi provenienti possono finire automaticamente nella posta indesiderata. Avete provato a bloccare l'incessante flusso di email di marketing da parte di Microsoft? Non si può.

4. Software applicativi - Gli utenti di Internet Explorer forse si aspettavano che il programma incorporasse una semplice gestione dei cookie e il blocco delle finestre a comparsa. Dopotutto sono cose che altri browser gestiscono tranquillamente, e che gli utenti hanno trovato molto utili per combattere varie seccature navigando in Internet. Ma Microsoft non sta soltanto vendendovi del software, vende anche pubblicità in Internet. Dunque non è nei migliori interessi dell'azienda offrire agli utenti delle funzionalità che potrebbero danneggiare i suoi partner in affari.

5. Spyware - Lo spyware altro non è che qualcuno che sta cercando di "possedere" il vostro computer. Questi programmi tengono traccia di ciò che fate sulla vostra macchina e lo trasmettono ai loro veri proprietari (a volte a vostra insaputa o senza il vostro permesso).

6. Update - Le caratteristiche di aggiornamento automatico sono un altro modo con il quale le aziende di software cercano di "possedere" il vostro computer. Se da un lato possono essere utili per migliorare la sicurezza, dall'altro richiedono la vostra fiducia nel rivenditore affinché non disattivi il vostro calcolatore per mancato pagamento, rottura di contratto o altre presunte infrazioni.

L'adware, il software-come-servizio e Google Desktop search sono tutti esempi del tentativo di altre aziende di "possedere" il vostro computer. Il Trusted Computing non farà altro che peggiorare la situazione.

Le tecnologie che tentano di "possedere" i computer altrui presentano un'insicurezza intrinseca: permettono a individui che non sono i legittimi proprietari dei computer di far rispettare delle policy su quelle macchine. Questi sistemi invitano gli aggressori ad assumere il ruolo della terza parte e di mettere un dispositivo contro il suo legittimo padrone.

Si tenga presente la vicenda Sony: la caratteristica più insicura di quel sistema DRM era un meccanismo di occultazione che permetteva al rootkit di controllare se fosse possibile o meno vederlo in esecuzione o individuare i suoi file sull'hard disk. Privandovi del possesso, diminuiva anche la vostra sicurezza.

Se lasciati crescere, questi sistemi di controllo esterno cambieranno radicalmente il nostro rapporto con il computer. Renderanno il nostro calcolatore molto meno utile, permettendo ad aziende e organizzazioni di limitarne i possibili utilizzi. Renderanno il nostro computer molto meno affidabile poiché non avremo più il controllo di ciò che si sta eseguendo sulla nostra macchina, di ciò che sta facendo, e di come i vari componenti software interagiscono fra loro. Portando l'esempio all'estremo, trasformeranno i nostri computer in gran bei televisori.

È possibile contrastare queste tendenze soltanto servendosi di software che rispetta i limiti da noi imposti. Boicottate quelle compagnie che non servono onestamente i propri clienti, che non rivelano le proprie alleanze, che trattano gli utenti come risorse di marketing. Usate software open source, software creato e posseduto da utenti, che non hanno secondi fini, alleanze segrete o accordi di marketing dietro le quinte.

Solo perché i computer rappresentavano una forza liberatrice in passato, non è detto che continuino a esserlo in futuro. Vi è un grandissimo potere politico ed economico dietro al concetto secondo cui non dovremmo realmente essere proprietari del nostro computer o del software che possediamo, pur avendo pagato per averlo.

Questo articolo è originariamente apparso su Wired.com:
<<http://www.wired.com/news/columns/1,70802-0.html>>

Il Trusted Computing:
<<http://www.schneier.com/crypto-gram-0208.html#1>>

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

Le ristampe di Crypto-Gram

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

<http://www.schneier.com/crypto-gram-back.html>. Quella che segue è una selezione di articoli apparsi in questo mese gli anni scorsi (le corrispondenti traduzioni in italiano le potete trovare all' indirizzo <http://www.cryptogram.it>, ndt).

REAL-ID

<http://www.schneier.com/crypto-gram-0505.html#2>

È giusto che i media parlino di terrorismo?

<http://www.schneier.com/crypto-gram-0505.html#3>

Combattere lo Spam

<http://www.schneier.com/crypto-gram-0505.html#15>

I mandati come misure di sicurezza:

<http://www.schneier.com/crypto-gram-0405.html#1>

Consumatori della Sicurezza Nazionale:

<http://www.schneier.com/crypto-gram-0405.html#9>

Crittografia e intercettazioni telefoniche:

<http://www.schneier.com/crypto-gram-0305.html#1>

Indirizzi e-mail specifici e Spam:

<http://www.schneier.com/crypto-gram-0305.html#6>

Segretezza, Sicurezza e Oscurità:

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

Ingannare i rilevatori di impronte digitali:

<http://www.schneier.com./crypto-gram-0205.html#5>

Che cosa può insegnare alla Sicurezza della Rete la Storia Militare, Seconda Parte:

<http://www.schneier.com/crypto-gram-0105.html#1>

L'inutilità della protezione dalla copia digitale:

<http://www.schneier.com/crypto-gram-0105.html#3>

Standard per la sicurezza:

<http://www.schneier.com/crypto-gram-0105.html#7>

Utilizzo sicuro del personal computer:

<http://www.schneier.com/crypto-gram-0105.html#8>

Sicurezza informatica: quando impareremo?

<http://www.schneier.com/crypto-gram-0005.html#1>

Trusted Client Software:

<http://www.schneier.com/crypto-gram-0005.html#6>

Il virus IL*VEYOU (titolo espurgato per evitare i filtri e-mail):

<http://www.schneier.com/crypto-gram-0005.html#ilyvirus>

L'internazionalizzazione della Crittografia:

<http://www.schneier.com/crypto-gram-9905.html#international>

La scoperta britannica della crittografia a chiave pubblica:

<http://www.schneier.com/crypto-gram-9805.html#nonsecret>

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

Leggi sulla divulgazione in caso di furto d'identità

Lo stato della California è stato il primo ad approvare una legge che obbliga le aziende che conservano dati personali a divulgare la notizia in caso tali dati vengano perduti o rubati. In seguito, molti altri stati hanno seguito l'esempio. Ora il Congresso sta discutendo una legislazione federale che applicherebbe il medesimo principio a livello nazionale.

Il problema è che non applicherà il medesimo principio: la legge federale è diventata così moderata che non risulterà essere molto efficace. Sarei comunque a favore di essa (una modesta legge federale è sempre meglio di niente), se non mandasse anche a vuoto altre leggi statali più efficienti, il che la rende un disastro completo.

Il furto d'identità è oggi un'area del crimine in rapidissima espansione. La denominazione è impropria (l'unica cosa che non vi può essere rubata è l'identità) ed è meglio definita come frode per sostituzione di persona. Un criminale raccoglie sufficienti informazioni sul vostro conto in modo da potersi sostituire a voi rapportandosi con le banche, le compagnie di carte di credito, i broker, ecc. Facendosi passare per voi, egli ruba i vostri soldi o semplicemente si diverte con il vostro credito a vostre spese.

Molte aziende conservano enormi database di informazioni personali che si rivelano assai utili per questi frodatori. Ma dato che tali compagnie non si sobbarcano il costo della frode, non sono incentivate economicamente a garantire una buona sicurezza per quei database. Infatti, se i vostri dati personali vengono sottratti dai loro database, tali aziende preferiscono di gran lunga non informarvi nemmeno: perché gestire la conseguente cattiva pubblicità?

Le leggi sulla divulgazione costringono le aziende a rendere pubbliche queste falle di sicurezza. Si tratta di un'ottima idea, per tre ragioni. La prima: è una buona pratica di sicurezza informare le potenziali vittime di furti d'identità che le loro informazioni personali sono andate perdute o rubate. La seconda: le statistiche sui veri e propri furti di dati sono preziose ai fini di ricerca. E la terza è che il costo potenziale della notifica e della conseguente cattiva pubblicità spinge naturalmente le varie aziende a investire più denaro sulla protezione di informazioni personali, o anche a non raccoglierne del tutto.

Si pensi a tutto questo come a un pubblico disonore. Le compagnie investiranno denaro per evitare i costi delle pubbliche relazioni per far fronte a tale disonore, e la sicurezza migliorerà. In termini economici, la legge diminuisce le esternalità e costringe le aziende a fare i conti con i costi reali di queste sottrazioni di dati.

Questo pubblico disonore necessita della cooperazione della stampa e, purtroppo, stiamo assistendo a un effetto di attenuazione. La prima grande violazione dopo che la California fece entrare in vigore la sua legge sulla divulgazione (la SB1386), accadde nel febbraio 2005, quando ChoicePoint vendette a dei criminali i dati personali di 145.000 persone. L'evento fece il giro delle news, e ChoicePoint fu costretta a migliorare la propria sicurezza.

In seguito, LexisNexis espose i dati personali di 300.000 persone, e Citigroup perse i dati di 3,9 milioni di individui. La legge SB1386 funzionò: se si è venuti a conoscenza di queste violazioni di sicurezza è stato grazie a quella legge. Ma tali violazioni si sono susseguite sempre più di frequente, e sempre di maggior entità. Dopo un certo periodo non facevano più notizia. E quando la stampa ha smesso di riportare questi eventi, il "costo" delle violazioni per le aziende è diminuito.

Oggi, l'unico vero costo rimasto è quello relativo alla notifica dei clienti e all'emissione di nuove carte. Alle banche l'emissione di una carta nuova costa circa 10 dollari, e si tratta di denaro che preferirebbero sicuramente non spendere. Questa è l'agenda che hanno introdotto nella legge federale, astutamente chiamata Data Accountability and Trust Act, o DATA.

I lobbisti hanno contrastato la legislazione in due modi. In primo luogo si sono attaccati alla definizione di informazioni personali. Solo l'esposizione di informazioni molto specifiche richiede la divulgazione. Per esempio, il furto di un database che contenesse l'iniziale del nome, il secondo nome, il cognome, il numero di Previdenza Sociale, il numero di conto bancario, l'indirizzo, il numero di telefono, la data di nascita, il nome da nubile della madre e la password, non sarebbe passibile di divulgazione, perché con "informazioni personali" si intende "il nome (per intero) e il cognome di una persona, congiuntamente a..." tutta una serie di altri dati personali.

In secondo luogo i lobbisti si sono attaccati alla definizione di "violazione della sicurezza". Nell'ultima versione della legge è scritto: "Il termine 'violazione della sicurezza' significa un'acquisizione non autorizzata di dati in formato elettronico contenenti informazioni personali tale da implicare una base ragionevole per stabilire l'esistenza di un rischio significativo di furto di identità ai danni degli individui cui tali informazioni personali si riferiscono".

Capito? Se un'azienda smarrisce un nastro di backup contenente le informazioni personali di milioni di individui, non è tenuta a divulgare la notizia se ritiene che non vi sia un "rischio significativo di furto di identità". Se una compagnia lascia esposto un database, e non possiede assolutamente alcun log che tenga traccia degli accessi a quel database, potrebbe dichiarare di non avere "basi ragionevoli" per stabilire l'esistenza di un rischio significativo. Addirittura potrebbe far riferimento a uno studio di ID Analytics che ha dimostrato che la probabilità di frode ai danni di una persona vittima di questo genere di perdita di dati è dell'ordine di 1 su 1.000, il che non rappresenta un "rischio significativo", e quindi l'azienda potrebbe non divulgare affatto la violazione e il furto di dati subito.

Ancora peggio, questa legge federale manda a vuoto le 23 leggi statali già esistenti più altre in via di considerazione, molte delle quali contengono protezioni individuali più forti. Pertanto, se può sembrare che DATA sia una legge a protezione dei consumatori a livello nazionale, in realtà è una legge che protegge le compagnie con grandi database ***dalle*** leggi statali a protezione dei consumatori.

Quindi, nella sua forma attuale, tale legislazione andrebbe a peggiorare le cose, non a migliorarle.

Ovviamente le cose sono in continuo cambiamento. Sono ***sempre*** in continuo cambiamento. Il linguaggio della legge è stato modificato regolarmente nel corso degli ultimi 12 mesi, con il susseguirsi delle varie commissioni che se ne sono occupate. Vi è anche un'altra legge, la

HR3997, che è ancora peggiore. E anche se venisse approvato qualcosa, dovrà essere conciliato con ciò che sarà approvato dal Senato, e quindi tornerà ai voti. Pertanto nessuno può davvero dire con quale tipo di linguaggio si esprimerà la legge in definitiva.

Ma il diavolo è nei dettagli, e l'unico modo per proteggerci da lobbisti che si mettono a giocherellare con i dettagli è quello di assicurarci che la legge federale non vanifichi nessuna legge statale: che la legge federale sia un minimo, ma che i singoli stati possano varare procedimenti più severi.

Detto questo, la divulgazione è importante, ma da sola non risolverà il problema del furto d'identità. Come ho scritto in precedenza, il motivo per cui il furto di informazioni personali è così diffuso è che quei dati sono preziosi. Il sistema per attenuare il rischio di frode per sostituzione di persona non è far sì che le informazioni personali siano più difficili da rubare, ma è il far sì che siano più difficili da sfruttare.

Le leggi sulla divulgazione affrontano soltanto l'esternalità economica di data broker che proteggono le vostre informazioni personali. Ciò di cui abbiamo realmente bisogno sono leggi che proibiscano alle compagnie di carte di credito e ad altre istituzioni finanziarie di garantire un credito a chiunque presenti poco più di un nome e un minimo di autenticazione.

Fino al momento in cui ciò accadrà, possiamo almeno sperare che il Congresso si astenga dall'approvare leggi che soppiantano ottime legislazioni statali e che finiscono col venire incontro ai criminali.

La legge californiana (SB 1386):

http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html oppure <http://tinyurl.com/dgh0>

Le leggi già esistenti sulla divulgazione:

<http://www.pirg.org/consumer/credit/statelaws.htm>

<http://www.cwalsh.org/cgi-bin/blosxom.cgi/2006/04/20#breachlaws>

HR 4127 - Data Accountability and Trust Act:

<http://thomas.loc.gov/cgi-bin/query/C?c109:./temp/~c109Xvx76>

HR 3997:

<http://thomas.loc.gov/cgi-bin/query/C?c109:./temp/~c109gnLQGA>

Lo studio di ID Analytics:

http://www.idanalytics.com/news_and_events/20051208.htm

Il mio intervento sul furto d'identità:

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

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

<http://www.wired.com/news/columns/0,70690-0.html>

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

Quando "Off" non significa "spento"

Secondo le specifiche della nuova Nintendo Wii (la nuova console di Nintendo per i giochi), "Wii può comunicare con Internet anche quando la console è spenta". Nintendo pone l'accento sui lati positivi: "Il servizio WiiConnect24 mette a disposizione una sorpresa o

l'aggiornamento di un gioco anche se gli utenti non stanno utilizzando Wii", ignorando la possibilità che Nintendo possa, volendo, disattivare un gioco, o che qualcun altro possa inviare tutto un altro genere di sorpresa, di certo poco gradita.

Lo sappiamo tutti, ma quel che è interessante in questo caso è che Nintendo sta cambiando il significato della parola "off", "spento". Siamo tutti portati a credere che "spento" vuol dire spento, e quindi sicuro. Ma nel caso di Nintendo "off" ha un significato più affine a "standby". Se gli utenti vogliono davvero disattivare Nintendo Wii, devono staccare la spina, assumendo che non vi sia una batteria che neutralizzi tale mossa. Sembra che non ci sia modo per scollegarsi da Internet, visto che Nintendo Wii è solo wireless.

Magari non c'è modo di spegnere Nintendo Wii.

Qui siamo in presenza di un grave problema di sicurezza, reso ancor peggiore da una pessima interfaccia utente. "Off" dovrebbe davvero significare "spento".

<http://wii.nintendo.com/hardware.html>

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

News

È un titolo di prima pagina provocatorio: "Gli aggiornamenti a Triple DES potrebbero introdurre nuove vulnerabilità nei Bancomat". In sostanza, i proprietari dei Bancomat stanno aggiornando la loro crittografia a Triple DES nello stesso momento in cui stanno passando a Internet i link delle comunicazioni ora presenti su linee dedicate. E mentre il protocollo cripta i PIN, non cripta invece il resto delle informazioni, come i numeri delle carte e le date di scadenza. Pertanto è il passaggio da linee dedicate a Internet a far aumentare le insicurezze, non gli aggiornamenti a Triple DES.

http://www.paymentsnews.com/2006/04/redspin_triple_.html

Un individuo ha compilato moduli di cambio d'indirizzo all'ufficio postale per dirottare al suo indirizzo la posta di altre persone. Lo ha fatto 170 volte. "Il portavoce del Servizio Postale, Patricia Licata, ha dichiarato che è richiesta una carta di credito per ragioni di sicurezza. 'Vi sono dei sistemi installati per evitare questo genere di eventi', ha affermato, ma si è astenuta dal commentare ulteriormente sul caso in questione finché i pubblici ufficiali non avranno stabilito che cosa è accaduto". Pare che quei sistemi non funzionino molto bene.

http://www.wvec.com/news/local/stories/wvec_local_041306_mail_scam.312100f4.html

Un esempio di deniable file system:

http://www.schneier.com/blog/archives/2006/04/deniable_file_s.html

Un'eccellente video burla, graffiti sull'Air Force One:

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

<http://abcnews.go.com/Technology/wireStory?id=1875386>

Il Dipartimento per la Sicurezza Nazionale ha rilasciato una "Request for Proposal" (richiesta di proposta, ossia un documento che chiede all'industria se qualcuno è in grado di fare ciò che viene richiesto) per la Secure Border Initiative.

http://www.washingtontechnology.com/news/1_1/daily_news/28381-1.html

Stuntz e Solove discutono su Privacy e Trasparenza.

<http://www.tnr.com/user/nregi.mhtml?i=20060417&s=stuntz041706>
<http://www.concurringopinions.com/archives/2006/04/william_stuntzs.html#more> oppure <<http://tinyurl.com/o4jte>>
<<http://www.tnr.com/user/nregi.mhtml?i=20060417&s=stuntz041706>>
<http://www.concurringopinions.com/archives/2006/04/stuntz_responds.html>
>
oppure <<http://tinyurl.com/mqrzt>>

Un'informazione utile per terroristi in viaggio: "Mio figlio e io ci siamo alzati domenica mattina e abbiamo guidato un camion a noleggio verso New York per spostare tutta la sua roba in un appartamento laggiù. Una volta arrivati all'Holland Tunnel, dopo aver attraversato la tratta Tony Soprano della Jersey Turnpike, la signorina del casello ci ha informati che, dall'11 settembre 2001, non è consentito il transito ai camion nell'Holland Tunnel; bisogna invece passare dal Lincoln Tunnel, ci ha detto. Perciò, se siete un terrorista che sta cercando di entrare in New York dal Jersey, sappiate che dovrete servirvi del Lincoln Tunnel".

<<http://www.post-gazette.com/pg/06110/683563-294.stm>>

La scultura Kryptos è situata al centro del Quartier Generale della CIA a Langley, Virginia. Fu realizzata nel 1990 e contiene un rompicapo crittografato in quattro parti. Le prime tre parti sono state risolte, ma si è saputo che la soluzione per la seconda parte era scorretta, ed è stata risolta una seconda volta:

<<http://www.elonka.com/kryptos/CorrectedK2Announcement.html>>

<<http://www.wired.com/news/technology/0,70701-0.html>>

Maggiori informazioni sulla scultura:

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

<<http://www.elonka.com/kryptos/>>

L'URL del post sul mio blog:

<http://www.schneier.com/blog/archives/2006/04/the_kryptos_scu.html>

Un boss della mafia protegge i suoi dati con il cifrario Caesar.

<http://dsc.discovery.com/news/briefs/20060417/mafiaboss_tec.html>

Gli innumerevoli avvisi di sicurezza di Microsoft Vista:

<http://www.winsupersite.com/reviews/winvista_5308_05.asp>

Il problema della gran quantità di finestre di dialogo è che non offrono alcuna sicurezza. Gli utenti smettono di leggerle. Le considerano delle seccature, come un clic in più richiesto per attivare una funzione.

L'atto di passare oltre facendo clic si imprime nella memoria muscolare, e nel momento in cui è davvero importante far caso all'avviso, l'utente non se ne accorgerà nemmeno.

<<http://www.codinghorror.com/blog/archives/000571.html>>

<<http://west-wind.com/weblog/posts/4678.aspx>>

Queste finestre di dialogo non rappresentano una sicurezza per l'utente; sono invece un sistema per mettersi al riparo ***dall'utente***. Quando qualche malware distrugge il vostro sistema, Microsoft può ribattere:

"Voi avete permesso al programma di farlo, non è colpa nostra". Le finestre di avviso sono efficaci soltanto se l'utente può utilizzarle per prendere decisioni intelligenti. Altrimenti sono solo seccature. E sono seccature che non migliorano la sicurezza.

<<http://blogs.zdnet.com/Ou/?p=209>>

Le fotocamere digitali possiedono impronte digitali uniche:

<http://www.eurekalert.org/pub_releases/2006-04/bu-bur041806.php>

È una ricerca interessante, ma vi è un aspetto importante di questa impronta digitale che l'articolo non ha trattato: quanto è difficile da falsificare? È possibile analizzare 100 immagini di una data fotocamera e poi contraffare un'altra immagine preesistente in modo che sembri provenire da quella fotocamera? Io ritengo che una cosa del genere si

possa fare con relativa facilità.

I rapporti dei Kaspersky Labs sulle frodi a scopo di estorsione commesse utilizzando malware:

<http://www.viruslist.com/en/analysis?pubid=184012401#crypto>

Fra gli altri worm, l'articolo discute il worm GpCode.ac, che crittografa i dati mediante RSA a 56 bit (no, non è un errore di battitura). L'intero articolo è una lettura molto interessante.

Larry Beinhart enuncia una tesi interessante per l'eliminazione della gran parte della segretezza governativa.

<http://www.buzzflash.com/contributors/06/04/con06131.html>

Ciò che dice non è male, anche se suppongo che la questione sia un poco più complicata.

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

"Security Myths and Passwords" [I Miti della Sicurezza e le Password], di Gene Spafford:

<http://www.cerias.purdue.edu/weblogs/spaf/general/post-30>

C'era un codice nell'ordinanza del giudice sul caso di plagio del "Codice Da Vinci". È stato risolto fin troppo velocemente dopo essere stato scoperto, poiché il giudice ha fornito alcuni indizi davvero ovvi. Ma è possibile trovare informazioni qui:

http://www.schneier.com/blog/archives/2006/04/da_vinci_code_r.html

A proposito di "Codice Da Vinci", io vengo menzionato nel libro. Sul serio. Pagina 199 dell'edizione americana rilegata: "Da Vinci era stato un pioniere della crittografia, Sophie lo sapeva, ma raramente gli fu attribuito tale merito. Gli istruttori universitari di Sophie, presentando metodi di crittografia informatica per proteggere dati, apprezzavano moderni crittologi come Zimmermann e Schneier ma dimenticavano di dire che era stato Leonardo, molti secoli addietro, a inventare una delle prime forme rudimentali di crittografia a chiave pubblica". Proprio così: sono un dettaglio realistico di sfondo.

http://fishbowl.pastiche.org/2004/07/06/house_of_cards

Technology Review presenta un interessante articolo che tratta alcune delle tecnologie utilizzate dalla NSA nel suo programma di intercettazione senza mandato, alcune di esse provenienti dal programma TIA (Total Information Awareness) che era stato annullato tempo fa.

http://www.technologyreview.com/read_article.aspx?ch=infotech&sc=&id=16741&pg=1 oppure <http://tinyurl.com/ruafx>

Secondo John Dvorak, Internet Explorer è stato il più grosso sbaglio commesso da Microsoft. Di certo la sua decisione di integrare strettamente IE nel sistema operativo (una manovra anticoncorrenziale contro Netscape durante la "guerra dei browser") ha causato enormi problemi di sicurezza da cui Microsoft non si è ancora ripresa. Nemmeno con l'introduzione di Internet Explorer 7.

http://www.pcmag.com/print_article2/0,1217,a=176507,00.asp

Sicurezza nei fumetti: gli aggressori sono adattabili:

<http://www.comics.com/comics/hedge/archive/hedge-20060423.html>

Abbiamo parlato di denaro contraffatto, di biglietti di concerti contraffatti, di credenziali di polizia fasulle, e di finti dipartimenti di polizia. Questa è una storia che tratta di una azienda fasulla.

<http://www.iht.com/articles/2006/04/27/business/nec.php>

Verizon ha annunciato di aver attivato il sistema Access Overload Control (ACCOLC), che permette ad alcuni cellulari di avere accesso prioritario alla rete anche quando è sovraccarica. Pare che occorra

digitare una specie di codice sul tastierino del telefono. Mi domando quanto ci vorrà prima che qualcuno faccia un hack ai danni del sistema.
<<http://www.pcsintel.com/content/view/1293/0/>>

Una squadra di artificieri fa saltare un espositore di giornali, scambiando una pubblicità promozionale del nuovo film di Tom Cruise per una bomba. È successo davvero, non si possono inventare storie del genere.
<http://www.editorandpublisher.com/eandp/news/article_display.jsp?vnu_content_id=1002425411> oppure <<http://tinyurl.com/n3286>>

Arma d'assalto che non viene rilevata dalle macchine a raggi X:
<<http://www.promoinnovations.com/xray.htm>>

Un tizio denuncia Compaq per pubblicità ingannevole. Ha acquistato un computer perché era stato pubblicizzato come "completamente sicuro". Ma dopo aver commesso alcuni reati e dopo che l'FBI gli ha sequestrato il computer, l'agenzia federale è stata in grado di recuperare i suoi dati. Questo è ciò che ho detto nell'articolo: "Purtroppo, con ogni probabilità non si tratta di un grande caso. Costui è un uomo che non si attirerà molte simpatie. È meglio un imputato che ha acquistato il Compaq e poi, beh, un suo concorrente, o un suo impiegato un po' farabutto, o qualcuno che è penetrato nel suo ufficio, gli ha rubato i dati. Ecco, questo è un imputato molto più simpatico".
<<http://hartfordadvocate.com/gbase/News/content?oid=oid:153106>>

Un neonato vittima di furto di identità:
<<http://www.abcnews.go.com/US/story?id=155878&page=1>>

Gli improvvisatori di un gruppo teatrale a New York si sono vestiti da dipendenti di Best Buy e sono entrati in uno store, videoregistrando di nascosto il risultato della performance. La parte che preferisco: "Le guardie della sicurezza e i manager hanno cominciato a parlarsi convulsamente attraverso i loro walkie-talkie e auricolari. 'Il caso Thomas Crown! Il Caso Thomas Crown!', ha iniziato a strillare un dipendente. Erano preoccupati che stessimo utilizzando le nostre uniformi fasulle per inscenare un qualche genere di furto molto elaborato. 'Voglio ogni dipendente disponibile steso sul pavimento, ADESSO!'".
<http://www.improveverywhere.com/mission_view.php?mission_id=57>

Rubare auto servendosi di computer portatili:
<<http://www.leftlanenews.com/2006/05/03/gone-in-20-minutes-using-laptops-to-steal-cars/>> oppure <<http://tinyurl.com/mkr9s>>
<<http://slashdot.org/articles/06/05/03/1928256.shtml>>

Il rapper MC Plus+ ha scritto una canzone sulla crittografia, "Alice and Bob". Parla di DES, AES, Blowfish, RSA, SHA-1, e altro. E fa anche il mio nome!
<<http://www.cs.purdue.edu/homes/anavabi/mp3/MC%20Plus+%20-%20Algorhythms%20-%20Alice%20and%20Bob.mp3>>
oppure <<http://tinyurl.com/8jov2>>
Un articolo sul "geeksta rap".
<<http://www.wired.com/news/culture/0,1284,67970,00.html>>

Il Dipartimento per la Sicurezza Nazionale, in violazione dell'accordo stipulato con l'Europa, condivide i dati di passeggeri delle linee aeree europee.
<<http://www.aclu.org/privacy/spying/25335prs20060425.html>>

Shell ha sospeso il suo sistema di pagamento chip-and-pin nel Regno Unito, dopo che dei frodatori hanno rubato più di un milione di sterline. Ne parlo approfonditamente nel mio blog:

http://www.schneier.com/blog/archives/2006/05/shell_suspends.html

Secondo questo articolo, l'ultima grande minaccia terroristica sono aerei robot teleguidati. L'articolo innalza davvero il livello di sensazionalismo delle minacce da trama cinematografica.

<http://www.physorg.com/news66197469.html>

Un reporter trova una vecchia carta d'imbarco British Airways, e la utilizza per scoprire tutto il resto sulla persona che lo possedeva.

<http://www.guardian.co.uk/g2/story/0,,1766138,00.html>

Si notino le pressioni economiche: "Qui il problema è che si affida a un'organizzazione commerciale il compito di raccogliere dati per conto di un governo straniero, per la qual cosa non ottiene alcuna ricompensa economica, e che non offre in cambio nessun vantaggio commerciale", afferma Laurie. "Ovviamente, in un caso del genere, cercheranno di ridurre i loro costi, e lo fanno girando il problema ai passeggeri stessi. Ciò, inoltre, ha come ottimo effetto collaterale quello di scaricare ogni responsabilità in caso di errori nei dati".

Cinque storie di hacking RFID:

<http://www.wired.com/wired/archive/14.05/rfid.html>

IBM pensa di avere la soluzione: una linguetta removibile che riduce il raggio del chip RFID:

<http://wired.com/news/technology/0,70793-0.html>

Perché non disabilitarlo del tutto?

Gravi problemi informatici all'interno della NSA:

<http://www.baltimoresun.com/news/custom/attack/bal-te.nsa26feb26,0,6311175.story> oppure <http://tinyurl.com/rgrso>

Nel frattempo la NSA sta costruendo uno smisurato database di analisi di traffico basato sui pattern di chiamata dei cittadini americani:

http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm

http://www.prospect.org/weblog/2006/05/post_336.html#002317

<http://glenngreenwald.blogspot.com/2006/05/no-need-for-congress-no-need-for.html>

<http://www.orinkerr.com/2006/05/11/thoughts-on-the-legality-of-the-latest-nsa-surveillance-program/>

<http://www.orinkerr.com/2006/05/12/more-thoughts-on-the-legality-of-the-nsa-call-records-program/>

Una grave vulnerabilità è stata trovata nelle macchine Diebold per il voto elettronico. Si tratta di un problema serio.

http://www.insidebayarea.com/ci_3805089

<http://www.blackboxvoting.org/BBVtsxstudy.pdf>

Un confronto fra la sicurezza delle macchine per il voto elettronico e la sicurezza delle slot machine:

<http://www.washingtonpost.com/wp-dyn/content/graphic/2006/03/16/GR2006031600213.html>

oppure <http://tinyurl.com/gda98>

Un ladro si traveste da guardia di museo e ottiene 200.000 Euro ingannando i dipendenti:

http://today.reuters.com/news/articlenews.aspx?type=oddlyEnoughNews&storyid=2006-05-03T204308Z_01_L02306327_RTRUKOC_0_US-ITALY-THIEF.xml

oppure <http://tinyurl.com/j3q6k>

Un affascinante racconto in prima persona sull'esperienza di essere nella watch list della TSA:

<http://arstechnica.com/news.ars/post/20060506-6767.html>

Reinterpretare l'intelligence nazionale:

<http://www.fas.org/blog/secretcy/2006/05/curing_analytic_pathologies.htm
> oppure <<http://tinyurl.com/lc2of>>

Crittografia a chiave pubblica per la legalizzazione notariale digitale in Pennsylvania.

<<http://www.nationalnotary.org/news/index.cfm?Text=newsNotary&newsID=851>
> oppure <<http://tinyurl.com/r9z4w>>
<<http://www.eweek.com/article2/0,1895,1955701,00.asp>>

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

Schede RFID e attacchi di tipo Man-in-the-Middle

Recenti articoli riguardanti la proposta di un documento di viaggio Stati Uniti-Canada e Stati Uniti-Messico (una specie di passaporto, ma meno utile), con incorporato un chip RFID che può essere letto a una distanza di circa 8 metri, hanno ancora una volta portato in primo piano la sicurezza RFID.

Le mie opinioni in proposito non sono mutate. La soluzione più sicura è una smart card che funzioni soltanto a contatto con un lettore; RFID è molto più rischioso. Ma se non abbiamo altro che lo RFID, allora la combinazione di isolamento del chip, misure di sicurezza di base per il controllo degli accessi, e una qualche azione da parte dell'utente per attivare il chip, può risultare buona. Il diavolo è nei dettagli, naturalmente, ma quelli elencati sono ottimi punti di partenza.

Quando si propongono chip con un raggio di lettura di 8 metri, occorre preoccuparsi degli attacchi di tipo man-in-the-middle. Un aggressore, di fronte a un lettore ufficiale, potrebbe "impersonare" la scheda di una persona nelle vicinanze, semplicemente inoltrando i messaggi da e verso la scheda di quella persona.

Ecco come funzionerebbe l'attacco. In questo scenario, Alice, funzionario di frontiera, possiede il lettore delle schede. Bob è il viaggiatore innocente, in coda a un qualche posto di frontiera. Mallory è l'aggressore, più avanti di Bob nella medesima fila alla frontiera, che si sostituirà a Bob davanti ad Alice. L'attrezzatura di Mallory comprende un lettore e trasmettitore RFID.

Supponiamo che la scheda debba essere attivata in qualche modo. Magari è necessario aprire il porta-documenti, oppure la scheda deve essere estratta da una custodia. Magari la scheda ha un pulsante che serve ad attivarla. Supponiamo inoltre che la scheda abbia un qualche protocollo di sicurezza challenge-response e un qualche protocollo per lo scambio delle chiavi.

1. Il lettore di Alice invia un messaggio al chip RFID di Mallory.
2. Il lettore/trasmettitore di Mallory riceve il messaggio e lo ritrasmette al chip di Bob (Bob è da qualche altra parte, fuori dal raggio di azione di Alice).
3. Il chip di Bob risponde normalmente al messaggio valido proveniente dal lettore di Alice. Non può sapere in alcun modo che è stato Mallory a inoltrare il messaggio.
4. Il lettore/trasmettitore di Mallory riceve il messaggio di Bob e lo ritrasmette ad Alice. Alice non ha modo di sapere che il messaggio è stato dirottato e re-inoltrato.

Il sistema di screening inserisce immagini test sullo schermo. Di solito il software fa lampeggiare le parole "Questa è una prova" sul monitor dopo un breve ritardo, ma questa volta il software non lo ha segnalato. Lo screener ha notato l'immagine (di un "dispositivo sospetto", secondo la CNN) e, secondo la procedura, gli addetti allo screening hanno controllato manualmente i bagagli sul nastro trasportatore alla ricerca di tale dispositivo. Naturalmente non hanno trovato nulla, ma hanno fatto evacuare l'aeroporto per due ore, cercandolo invano.

Hartsfield-Jackson è uno degli aeroporti più affollati e attivi del paese. È il cuore della compagnia Delta. I ritardi sono stati sentiti in tutto il paese per il resto della giornata.

Bene, dunque che cosa è andato storto in questo caso? Chiaramente è stato un malfunzionamento del software. Altrettanto chiaramente non è stato un errore delle procedure degli addetti allo screening: tutti hanno fatto ciò che dovevano.

Quel che risulta meno ovvio è che è stato il sistema ad aver fallito. Ha fallito perché non è stato progettato per fallire bene. Un piccolo errore, in questo caso un'anomalia software di un'unica macchina a raggi X, ha portato a un effetto-valanga al punto di dover chiudere l'aeroporto. Questo genere di amplificazione dell'errore è comune in molti sistemi di sicurezza mal progettati. Meglio sarebbe sistemare singole macchine a raggi X ai vari gate (ho visto questa soluzione in molti aeroporti europei), così che in presenza di un problema, gli effetti sono limitati a quel gate.

Naturalmente, tale soluzione di sicurezza distribuita sarebbe anche più costosa. Ma scommetto che finirebbe col risultare più economica, se consideriamo i costi delle occasionali evacuazioni di un intero aeroporto.

<http://www.cnn.com/2006/US/04/20/atlanta.airport/index.html>

Ciò che scrissi il mese scorso:

http://www.schneier.com/blog/archives/2006/03/airport_passeng.html

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

Le News di Counterpane

Il 23 maggio Schneier aprirà una serie di conferenze dell'ACLU con una lezione su "Il Futuro della Privacy".

<http://www.aclu.org/privacy/25551res20060512.html>

Schneier interverrà al Gartner IT Security Summit a Washington DC il 5-7 giugno:

http://www.gartner.com/2_events/conferences/sec12.jsp

Schneier interverrà alla ACLU New Jersey Membership Conference:

<https://www.aclu-nj.org/events/aclunjmembershipconference>

Schneier interverrà alla ACLU Vermont Privacy Conference:

<http://www.acluvt.org/news/display.php?sid=1145047166&PHPSESSID=31bdcef418904b0caablffbdelf8a64> oppure <http://tinyurl.com/pdzyy>

Tipping Point sta offrendo servizi di Managed Security tramite un'alleanza con Counterpane:

<http://www.counterpane.com/pr-20060501.html>

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

Microsoft BitLocker

BitLocker Drive Encryption è una nuova caratteristica di sicurezza di Windows Vista, ideata per funzionare congiuntamente al Trusted Platform Module (TPM). In sostanza cripta l'unità C: con una chiave generata dal computer. Nella sua modalità base, un aggressore potrebbe sempre accedere ai dati sul disco indovinando la password dell'utente, ma non sarebbe in grado di accedere al disco facendo il boot da un altro sistema operativo, né togliendo il disco e collegandolo a un altro computer.

BitLocker ha diversi modi di funzionamento. Nella modalità più semplice, il TPM conserva la chiave e il tutto avviene in maniera totalmente invisibile. L'utente non deve fare nulla di diverso dal solito, né nota nulla di diverso.

La chiave di BitLocker può anche essere conservata in un disco USB. In questo caso l'utente deve inserire il disco USB nel computer durante l'avvio. Poi vi è una modalità che si serve di una chiave conservata nel TPM e di una chiave archiviata in un disco USB. E infine vi è un'altra modalità che sfrutta una chiave nel TPM e un PIN di quattro cifre che l'utente immette nel computer. Tutto questo avviene all'inizio del processo di avvio, quando vi sono ancora caratteri ASCII a video.

Si noti che se si configura BitLocker con una chiave USB o un PIN, il metodo di indovinare la password non funziona. BitLocker non permette nemmeno di giungere a una schermata di richiesta password.

Per la maggior parte delle persone, la modalità base è la migliore. Molte persone terranno la loro chiave USB nella borsa insieme al loro portatile, per cui non vi sarà molta sicurezza aggiunta. Ma se fosse possibile indurre gli utenti ad attaccarla al proprio portachiavi (si ricordi che la chiave serve soltanto ad avviare il computer, non a farlo funzionare) e convincerli a inserirla nel proprio computer ogni volta che lo avviano, allora si otterrebbe un livello di sicurezza maggiore.

Vi è una chiave di recupero: facoltativa ma caldamente raccomandata. Viene generata automaticamente da BitLocker, e può essere inviata a un amministratore o stampata e conservata in qualche luogo sicuro. Sono a disposizione di un amministratore delle funzioni per impostare policy di gruppo che richiedano questa chiave.

Tuttavia non vi sono backdoor per la polizia.

È possibile far funzionare BitLocker su sistemi privi di TPM, ma è scomodo. Si può solo configurarlo per una chiave USB. E funzionerà solo con certo hardware: dato che BitLocker si avvia prima che venga caricato qualsiasi driver, il BIOS deve riconoscere le unità USB affinché BitLocker possa entrare in azione.

Dettagli sulla crittografia: l'algoritmo di default di criptazione dei dati è AES-128-CBC con un diffusore (diffuser) aggiuntivo. Il diffusore è progettato per proteggere da attacchi di manipolazione del ciphertext, ed è introdotto indipendentemente da AES-CBC così da non poter danneggiare la sicurezza che si ottiene da AES-CBC. Gli amministratori possono impostare l'algoritmo di crittografia del disco attraverso policy di gruppo. Le opzioni sono: AES-CBC a 128 bit più il diffusore, AES-CBC a 256 bit più il diffusore, AES-CBC a 128 bit e AES-CBC a 256 bit. (Il mio consiglio: lasciare il valore di default). Il sistema di

gestione della chiave utilizza chiavi a 256 bit ove possibile. L'unico luogo in cui il limite a 128 bit viene fissato a livello hardware è la chiave di recupero, che è di 48 cifre (checksum compresi). È più corta perché deve essere inserita manualmente; inserire 96 cifre farebbe imbestialire molta gente, anche se fosse solo per il recupero dei dati.

Questa procedura distruggerà i sistemi dual boot? Non proprio. Se Vista è in esecuzione, e poi si cerca di impostare un sistema dual boot, BitLocker considererà tale cambiamento come un attacco e si rifiuterà di funzionare. Ma poi è possibile utilizzare la chiave di recupero per fare il boot in Windows e quindi istruire BitLocker ad accettare la configurazione attuale (con il codice dual boot). Dopodiché il sistema dual boot sarà tranquillamente utilizzabile, almeno così mi è stato detto. Non sarà possibile condividere alcun file dell'unità C: fra i diversi sistemi operativi, ma si potranno condividere i file di qualunque altra unità.

Il problema è che è impossibile distinguere fra un sistema dual boot legittimo e un aggressore che sta cercando di sfruttare un altro sistema operativo (Linux o un'altra istanza di Vista) per arrivare al disco principale.

BitLocker non è un sistema DRM. Tuttavia è molto semplice trasformarlo in un sistema DRM. Basta dare ai programmi la capacità di richiedere che i file vengano archiviati solamente su dischi abilitati da BitLocker, e che siano trasferibili solo ad altre unità abilitate da BitLocker. Quanto questo sia semplice da implementare e arduo da sconvolgere dipende dai dettagli del sistema.

BitLocker non è neanche una panacea, tuttavia attenua un rischio particolare ma importante: il rischio che degli aggressori abbiano accesso diretto ai dati su disco. Permette quindi di gettare via o di vendere vecchi hard disk senza problemi. Fa in modo che la gente smetta di preoccuparsi che i propri dischi vadano perduti o vengano rubati. Blocca un tipo specifico di attacco contro i dati.

Al momento BitLocker si trova solo nelle versioni Ultimate e Enterprise di Vista. È una feature disattivata per default. Si tratta anche della prima applicazione TPM di Microsoft. Presumibilmente verrà ampliata in futuro: permettere la crittografia di altri dischi e unità sarebbe un ottimo passo successivo, per esempio.

<http://www.microsoft.com/technet/windowsvista/library/help/b7931dd8-3152-4d3a-a9b5-84621660c5f5.mspx?mfr=true> oppure <http://tinyurl.com/fywd7>
<http://www.microsoft.com/technet/windowsvista/library/c61f2a12-8ae6-4957-b031-97b4d762cf31.mspx> oppure <http://tinyurl.com/h4nc8>

Niels Ferguson sulle backdoor:
http://blogs.msdn.com/si_team/archive/2006/03/02/542590.aspx

BitLocker e i sistemi dual boot:
http://www.theregister.co.uk/2006/04/27/schneier_infosec/
<http://arstechnica.com/journals/microsoft.ars/2006/4/28/3782>

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

I rischi di sicurezza dei casi particolari

In "Beyond Fear" ho parlato dei rischi di sicurezza intrinseci alle eccezioni di una policy di sicurezza. Ecco un esempio, dalla sicurezza

aeroportuale in Irlanda.

Gli ufficiali di polizia hanno il permesso di passare oltre i checkpoint di sicurezza all'aeroporto di Dublino. Mostrano il loro tesserino e passano oltre.

“Una donna appartenente all'unità di sicurezza dell'aeroporto sta compiendo un nuovo addestramento a seguito di un incidente in cui un ispettore del Dipartimento dei Trasporti ha oltrepassato un checkpoint senza essere controllato.

“Pare che il funzionario del dipartimento sia stato fatto passare oltre i controlli di sicurezza dopo aver mostrato un tesserino identificativo. L'ispettore ha immediatamente informato le autorità aeroportuali di questo errore di omissione nelle procedure di verifica. Solo ai Gardai (ufficiali delle forze dell'ordine irlandesi) è permesso di passare ai checkpoint senza essere controllati”.

Questo errore può essere accaduto in due modi. 1) L'addetto alla sicurezza può aver pensato che i funzionari del Dipartimento dei Trasporti avessero gli stessi privilegi dei poliziotti. 2) L'addetto alla sicurezza può aver pensato che quel documento fosse un tesserino della polizia.

E avrebbe potuto benissimo trattarsi di un criminale che mostrava un finto tesserino di polizia. Mi è lecito supporre che gli addetti alla sicurezza non controllano questi documenti molto accuratamente.

Qui il punto è che le eccezioni alla sicurezza sono esse stesse vulnerabilità di sicurezza. Non appena si crea un sistema per cui alcune categorie di persone possono aggirare i checkpoint di sicurezza di un aeroporto, si invitano i criminali a tentare di sfruttare quel sistema. Chiaramente ci possono essere dei buoni motivi per creare percorsi alternativi attraverso la sicurezza, ma in tal caso occorre studiare bene i compromessi che ne derivano.

<http://archives.tcm.ie/businesspost/2006/04/16/story13502.asp>

** **

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.