

CRYPTO-GRAM
15 luglio 2003

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

Edizione italiana curata da Communication Valley SpA

e-mail: schneier@counterpane.com

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

** **

In questo numero:

[Come reagire](#)

[Il Canile: YTech](#)

[Altre idiozie dei filtri di posta elettronica](#)

[News](#)

[Le news di Counterpane](#)

[Note di sicurezza da ogni dove: il vino rosso](#)

[Password Safe](#)

[I falsi allarmi](#)

[Commenti dei lettori](#)

** **

Come reagire

Sono atterrato a Los Angeles alle 23:30, e mi ci è voluta un'altra ora prima di raggiungere l'hotel. Tutti gli alberghi della città erano esauriti, e sono stato fortunato ad avere una prenotazione in quell'hotel. Al mio arrivo, alla reception, l'impiegato ha insistito nel voler fare una fotocopia della mia patente di guida. Ho cercato di resistere, ma è stato inutile. Avevo bisogno della mia stanza. Non c'era altro posto in cui andare. All'impiegato del turno di notte non importava che io prendessi la stanza o meno. Aveva delle regole da seguire e le avrebbe seguite.

Mia moglie aveva bisogno di una ricetta medica. Il suo dottore ha dato istruzioni per telefono a una farmacia locale, e quando lei è passata a ritirarla, il farmacista si è rifiutato di compilarla a meno che lei non avesse comunicato i propri dati personali per il database della farmacia. Il farmacista ha persino mostrato a mia moglie il regolamento, e lei ha potuto trovare la parte in cui si dice che "la farmacia dovrebbe fare il possibile per ottenere, registrare e conservare almeno le seguenti informazioni", e la parte in cui si dice anche: "se un paziente è contrario alla creazione di un profilo personale, egli dovrà dichiararlo per iscritto al farmacista. In questo modo al farmacista non sarà richiesto di preparare un profilo come da prassi per tutti gli altri casi". Malgrado questo, il farmacista si è rifiutato. Mia moglie non sapeva che fare, era bloccata. Aveva bisogno della ricetta e non voleva aspettare il tempo necessario al suo medico per chiamare un'altra farmacia. Al farmacista non importava, ed era assolutamente inamovibile.

Lo scorso anno sono dovuto andare in Giappone, e ho trovato una società che affitta telefoni cellulari locali ai viaggiatori. Il modulo di richiesta obbliga ad inserire il numero di previdenza sociale oppure il numero di passaporto. Quando ho domandato all'impiegato il perché di questa procedura, mi ha risposto che l'assenza di una di queste informazioni avrebbe invalidato la

procedura. Gli ho chiesto quindi come avrebbe potuto distinguere un numero falso ma verosimile da uno assolutamente corretto. Lui mi ha risposto che se non era mia intenzione dare quel numero come richiesto, potevo benissimo rivolgermi a qualcun altro per l'affitto del cellulare, e mi ha attaccato il telefono in faccia. Allora mi sono rivolto ad un'altra società, ma si è poi scoperto che stipulavano contratti attraverso la stessa società che avevo in precedenza contattato, e il tizio si rifiutava di trattare con me, anche in via indiretta. Alla fine ho ottenuto il cellulare richiamando la prima società e dando un nome diverso (quello di mia moglie), un numero diverso di carta di credito, e un numero di passaporto fittizio. Situazione risolta e reputazione salvata per tutti, immagino.

È la stagione della sicurezza stupida. Se avete avuto occasione di volare, o di entrare in un edificio governativo, o di fare decine di altre cose, vi sarete sicuramente imbattuti in sistemi di sicurezza invasivi, controproducenti, grossolani o semplicemente fastidiosi. Avrete incontrato persone, quali guardie, funzionari, impiegati al minimo salariale, che vi hanno costretto a rispettare ciecamente le più stupide regole di sicurezza immaginabili.

C'è qualcosa che possiamo fare?

Alla fin fine, tutta la questione della sicurezza altro non è che un negoziato fra le parti in causa: governi, industrie, aziende, organizzazioni, singoli individui, ecc. Le varie parti decidono che genere di sicurezza vogliono e che cosa sono disposti a dare in cambio per ottenerla. Ma a volte pare proprio che noi, in qualità di individui, non siamo considerati come parte di quel negoziato. La sicurezza sembra più essere qualcosa che ci viene fatto subire.

La nostra sicurezza dipende in gran parte dalle azioni di altri e dall'ambiente in cui ci troviamo. Per esempio, la resistenza alla manomissione che possiedono le confezioni di cibo dipende più dalle regolamentazioni governative sul confezionamento che non dalle nostre scelte di acquisto. La sicurezza di una lettera inviata ad un amico dipende più dall'etica dei lavoratori che la maneggiano che non dalla marca delle buste che decidiamo di usare. Quanto un aereo sia sicuro da eventuali esplosioni ha molto poco a che vedere con ciò che facciamo in aeroporto e sull'aereo (lo "shoe-bomber" Richard Reid ha rappresentato una rara eccezione a questo). La sicurezza del denaro sul nostro conto in banca, il tasso di criminalità del nostro quartiere, e l'onestà e l'integrità dei nostri dipartimenti di polizia sono cose fuori dal nostro controllo diretto. Semplicemente, non abbiamo abbastanza potere nei "negoziati" per poter cambiare le cose.

Non ho avuto alcun potere quando ho cercato di avere la mia stanza all'hotel senza dover fornire la mia patente di guida. Mia moglie non ha avuto potere quando ha cercato di ottenere la sua ricetta medica senza dover divulgare un sacco di informazioni personali facoltative. L'unico motivo per cui ho avuto potere nell'affittare un cellulare in Giappone è perché ho deliberatamente ingannato il sistema. Se cerco di contestare la sicurezza delle compagnie aeree, perderò il mio volo di sicuro, e potrei perfino essere arrestato. Non c'è uguaglianza, perché coloro che implementano la sicurezza non hanno interesse a cambiarla, né il potere di farlo. Non sono loro a controllare il sistema della sicurezza; forse è meglio pensare a loro quasi come a dei robot senza cervello: il sistema della sicurezza si affida a questo modo di comportarsi, rimpiazzando la flessibilità e l'adattabilità del giudizio umano con un grosso faldone di procedure e di "best practices".

Le cose sarebbero diverse se il farmacista fosse il proprietario della farmacia, o se la persona dietro il bancone della reception fosse il proprietario dell'hotel. Anche se l'agente di polizia fosse il poliziotto di quartiere. In questi casi vi sarebbe più uguaglianza. Posso negoziare la mia sicurezza e l'altra persona può decidere se modificare le regole per me oppure no. Ma la società di oggi è sempre più spesso costituita da aziende senza volto e governi senza testa. È implementata da persone e macchine che hanno un enorme potere, ma solo il potere di implementare ciò che viene loro detto di implementare. Non hanno un vero interesse nel negoziare, non ne hanno bisogno e a loro non importa.

Ma esiste un paradosso. Noi non siamo solo individui, siamo anche consumatori, cittadini, contribuenti, elettori e -- se le cose peggiorano davvero -- contestatori e a volte anche folle inferocite. Solo nell'aggregazione abbiamo potere e più ci organizziamo, più potere abbiamo.

Anche il presidente di una compagnia aerea, nel farsi largo attraverso la sicurezza degli aeroporti, non ha potere per negoziare il livello di sicurezza che riceverà e i compromessi che è disposto a concedere. In un aeroporto e su un aereo, non siamo altro che passeggeri: una risorsa che deve essere protetta da un potenziale aggressore. Il solo modo per cambiare la sicurezza è quello di fare un passo fuori dal sistema e di negoziare con i singoli incaricati. È solo al di fuori del sistema che ognuno di noi ha potere: a volte come possessori di una risorsa, ma più spesso come altra parte in gioco ed è al di fuori del sistema che riusciremo a compiere le trattative migliori.

Fuori dal sistema abbiamo potere e possiamo negoziare con le persone che hanno potere sul sistema di sicurezza che vogliamo cambiare. Dopo il mio soggiorno all'hotel, ho scritto alla direzione dicendo che non sarei mai più tornato lì (purtroppo sto collezionando un lunghissimo elenco di hotel in cui non mi fermerò più). Mia moglie ha steso un reclamo contro quel farmacista presso il Minnesota Board of Pharmacy. John Gilmore sta facendo di più: si rifiuta di volare da dopo la tragedia dell'11 settembre e sta facendo causa al governo per il diritto costituzionale di viaggiare all'interno degli Stati Uniti senza dover mostrare una fototessera identificativa.

Tre punti per quanto riguarda il reagire. Primo, negoziare a confronto diretto -- cliente e proprietario della farmacia, ad esempio -- può essere efficace, ma comporta anche tutta una serie di fattori indesiderati come classe sociale e razza. È spiacevole a dirsi, ma terribilmente vero, che in un'eventuale trattativa con un poliziotto avrò maggiori probabilità di riuscita rispetto ad una persona di colore. Per questa ragione, reclami e rimostranze più formali saranno spesso più efficaci di un negoziato faccia a faccia.

Secondo, i rimproveri e gli insulti non funzionano. Così come non ha senso mettersi a discutere con un impiegato, non ha nemmeno senso insultarlo. Si dica invece: "so che lei non ha scritto le regole, ma nel caso chi le ha scritte le chiedesse se stanno funzionando, gli faccia sapere che i clienti pensano che siano stupide, offensive e inefficaci". Se da un lato è molto difficile cambiare la mentalità di una istituzione quando è nel bel mezzo di una disputa, dall'altro è possibile influenzare la discussione più generale. Altre aziende stanno prendendo le stesse decisioni in merito alla sicurezza e occorre far sapere loro che tutto questo non sta funzionando.

Terzo, non si dimentichi l'andamento politico. Le elezioni contano; la pressione politica esercitata da funzionari eletti sulle aziende e sulle agenzie governative possiede un reale impatto. Una delle forme di protesta più influenti è quella di votare per quei candidati che condividono i vostri ideali.

Più ci uniamo, più potere abbiamo. Un boicottaggio su larga scala di quelle strutture che richiedono una fototessera identificativa porterebbe ad un cambiamento. Chi organizza conferenze ha più influenza dei singoli individui sugli alberghi. Le conferenze USENIX non si serviranno di quegli hotel che richiedono documenti di identità agli ospiti, per esempio. Un folto gruppo di elettori a voto unico che sostenesse quei candidati che hanno lavorato contro un tipo di sicurezza stupido, farebbe la differenza.

Purtroppo, ritengo che le cose peggioreranno di molto prima di migliorare. Molte persone non sembrano infastidite dalla "stupida sicurezza"; alcuni si sentono persino più al sicuro. Negli Stati Uniti ormai la gente è abituata a mostrare ovunque un documento di identità; è la nuova realtà della sicurezza dopo l'11 settembre. Le persone sono abituate a questa sicurezza intrusiva e credono a coloro i quali ne affermano la necessità.

È importante scegliere bene le nostre battaglie. Credo che molti degli sforzi per combattere la sicurezza stupida siano sprecati. Nessun albergo ha cambiato i propri metodi a seguito delle mie infuocate lettere di protesta o di un calo della clientela. Una volta in tribunale, la causa di Gilmore sarà probabilmente e, sfortunatamente, persa. Mia moglie con ogni probabilità renderà la vita difficile a quel farmacista per un po', ma quel modo di procedere magari continuerà in tutte le farmacie della catena. Se dovessi avere ancora bisogno di un cellulare in Giappone, userò lo stesso trucco. Il ribellarsi potrebbe far sì che veniate marchiati come agitatori, il che porterebbe a maggiori problemi.

Però possiamo ancora farci sentire. La causa di Gilmore sta generando ogni genere di copertura da parte della stampa, e sta contribuendo ad una maggiore sensibilizzazione generale. La Boycott Delta campaign ha avuto un impatto vero e proprio: si sta rivedendo il metodo di stesura dei profili dei passeggeri a causa di pubbliche lamentele. A causa di agitazioni pubbliche, il programma Terrorism (Total) Information Awareness di Pointdexter, anche se non è stato ritirato, non sta attraversando un buon momento.

Quando vi capita di vedere un tipo di sicurezza controproducente, invasivo, o semplicemente stupido, non fate finta di niente. Scrivete una lettera. Create un sito Web. Compilate una richiesta per la libertà d'informazione (FOIA). Fate un po' di rumore. Non dovete sottoscrivere nulla o aggregarvi a nessuno; il rumore non dev'essere altro che degli individui che combattono per se stessi.

Non si vincerà ogni volta. Ma qualche volta sì.

I premi per la Stupida Sicurezza assegnati da Privacy International:
<<http://www.privacyinternational.org/activities/stupidsecurity/>>

Il blog sulla Stupida Sicurezza:
<<http://www.stupidsecurity.com/>>

Le aziende tirano in ballo la sicurezza per far sì che il governo dia loro tregua:
<http://online.wsj.com/article_email/0,,SB10541572621041000,00.html>

La causa di Gilmore:
<<http://freetotravel.org/>>

Le regole dei farmacisti relative allo stato del Minnesota:
<<http://www.revisor.state.mn.us/arule/6800/3110.html>>

Come potete essere d'aiuto ora:

Dite al Congresso di tenere sotto controllo il progetto per la sicurezza aerea:
<<http://actioncenter.ctsg.com/admin/adminaction.asp?id=2557>>

Aggiornamento sul TIA: chiedere ai propri senatori di sostenere il Data-Mining Moratorium Act del 2003:
<<http://actioncenter.ctsg.com/admin/adminaction.asp?id=2401>>

Il Congresso mira alla vostra privacy:
<<http://actioncenter.ctsg.com/admin/adminaction.asp?id=1723>>

Total Information Awareness: è l'ora delle udienze pubbliche!
<<http://actioncenter.ctsg.com/admin/adminaction.asp?id=2347>>

Non lasciate che l'INS violi la vostra privacy:
<<http://actioncenter.ctsg.com/admin/adminaction.asp?id=2436>>

Il 2 luglio, sia il Governo degli Stati Uniti, sia ISS (una compagnia che vende prodotti di sicurezza informatica) hanno comunicato una storia riguardante qualcosa chiamato "Defacers Challenge". Apparentemente, migliaia di siti web sarebbero stati sottoposti a defacement il 6 luglio, come parte di un certo gioco. La stampa ha raccolto questa storia, che è stata presto trasformata in scoop internazionale. Noi a Counterpane abbiamo considerato tutto questo un'assurdità, ma quando i nostri clienti hanno cominciato a chiamarci, abbiamo dovuto pubblicare un comunicato.

Il 6 di luglio è arrivato ed è passato, e non è accaduto nulla. Ritengo che si sia trattato di uno scherzo.

Non che avessimo potuto fare qualcosa in caso contrario. Molte delle notizie e dei comunicati dicevano alla gente di assicurarsi che le proprie misure di sicurezza fossero aggiornate e che le patch fossero tutte recenti. Questo è un buon consiglio per ogni giorno dell'anno. Preoccuparsi per il 6 luglio non ha fatto sì che i siti web fossero meno attaccabili del solito.

Per anni l'industria della sicurezza ha cercato di sopravvivere basandosi sul cosiddetto FUD: fear, uncertainty, doubt (cioè paura, incertezza, dubbio). L'idea di base è che se spaventate i vostri potenziali clienti, questi compreranno i vostri prodotti. L'avidità e la paura sono due delle molle principali che spingono l'uomo, ed entrambe vengono continuamente sfruttate dagli esperti di mercato delle aziende e del governo. Il problema è che il FUD funziona solo per un po'. Alla fine la gente capisce che non c'è nulla di cui preoccuparsi. Alla fine la gente ignora gli avvertimenti. Quando si arriva a quel punto, le persone non tengono conto né degli avvertimenti reali, né di quelli presunti.

Prevenire il FUD è difficile. Anche i più esperti fra noi hanno dovuto affrontare la storia della Defacers Challenge. Alcuni reporter ne hanno parlato perché è una specie di storiella interessante, e poi si sono aggiunti tutti gli altri. Ricordo di aver parlato con un reporter. Mi ha detto che all'inizio aveva ignorato la storia, capendo che si trattava di FUD. Ma quando altri giornali hanno cominciato ad occuparsene, il suo editore gli ha ordinato di scrivere qualcosa a riguardo. Non importava che non si trattasse di una notizia vera; era una notizia solamente perché altri ne parlavano.

In qualche strano modo, la stampa ha reso la minaccia reale. Migliaia di aspiranti defacer, che non avrebbero mai sentito di questa Defacers Challenge, lo hanno saputo dai giornali. "Sembra divertente", avranno pensato.

Di recente ho letto parecchi articoli riguardo al perché l'industria della sicurezza informatica sia in depressione. Pare che la gente non stia acquistando quei nuovi prodotti di sicurezza tanto belli e carini. Vi sono decine di ragioni per questo, ma il FUD è una delle principali. Abbiamo minacciato gli acquirenti parlando dei grossi pericoli di Internet. Abbiamo promesso agli acquirenti che -- stavolta per davvero -- i nostri prodotti avrebbero risolto tutti i loro problemi. Ma sapete che è successo? Che gli acquirenti si sono fatti più cinici. Hanno notato che non è poi così male, là fuori. Hanno notato che i problemi rimangono, sia che comprino, sia che non comprino i prodotti.

Ecco il mio suggerimento per chiunque cerchi di vendere la sicurezza informatica: dimostrate valore. Dimostrate il ritorno di investimento. Dimostrate che i vostri prodotti permettono ai vostri clienti di migliorare la gestione dei rischi. Il FUD non funziona più ormai. Non vende nulla, e non fa altro che irritare i possibili clienti.

Purtroppo, il Governo statunitense dovrà imparare questa stessa lezione. Dalla tragedia dell'11 settembre, il Dipartimento della Sicurezza Nazionale ha innalzato il livello di minaccia terroristica al colore arancio per due volte (credo). Ogni volta ci è stato detto di stare in guardia, ma di farci gli affari nostri. Ogni volta non è accaduto niente.

Commenti dei lettori

Da: Rob Lemos <robert.lemos@cnet.com>

Oggetto: Il cyber-terrorismo

Tutte le volte che parlo di cyber-terrorismo, dico che il consulente del Queensland, Vitek Boden, ha rilasciato un milione di litri di acque torbide in un estuario che è stato ripulito in una settimana. Un paio di mesi dopo, un uccellino si è posato su un trasformatore nella Ohio River Valley, ha fatto saltare se stesso e il trasformatore, e sono stati rilasciati circa 2,5 milioni di galloni (diciamo 10 milioni di litri) di acque fognarie nel fiume.

Quindi pare che ci si debba preoccupare più degli uccelli che degli hacker o, per essere meno irriverenti, degli attacchi fisici più che di quelli via Internet.

Da: Allan Dyer <adyer@yuikee.com.hk>

Oggetto: Insegnare a scrivere virus

Il problema non è insegnare come funzionano gli exploit, i virus e i worm, ma l'inutile creazione di codice auto-replicante. Abbiamo bisogno di più persone che siano in grado di capire e di combattere i virus, ma non è necessario creare un virus per questo. Inoltre, il saper creare un virus non significa affatto possedere tutta quella serie di capacità richieste per combatterli. Unitamente ai pericoli intrinseci legati al codice auto-replicante, ciò rende la pratica di scrivere virus superflua e immorale.

I pericoli intrinseci sono il risultato di tre proprietà del codice auto-replicante: la generalità, il raggio di effetto, e la persistenza. Queste cambiano il modo in cui dovremmo pensare alla sicurezza. In particolare, se falliscono le precauzioni prese per evitare la fuga di codice dal laboratorio, allora non c'è un limite predeterminato di quanto danno può causare, o di quanto tempo può sopravvivere. Così come sappiamo che non esistono garanzie assolute nell'ambito della sicurezza, chi organizza quei corsi dovrebbe quindi ridurre al minimo il potenziale del danno fornendo agli sviluppatori di antivirus tutti i campioni dei virus creati. I virus creati da un corso universitario ogni anno, diciamo 50 virus, non farà molta differenza nel numero totale dei nuovi virus: al momento ve ne sono di 50.000 tipi conosciuti. Tuttavia, se questo è un corso buono e utile, allora ogni università nel mondo dovrà avere un corso simile, e potremmo così iniziare a vedere 50.000 nuovi virus all'anno, solo grazie a questi corsi.

Insomma, è possibile studiare virus e worm senza crearne? La caratteristica che differenzia un virus da altri programmi è la capacità di modificare altri programmi per includere una copia di se stesso; ma, in termini di studio e comprensione di tecniche, che differenza c'è fra:

i) modificare il programma A per includere una copia del programma B.

ii) modificare il programma A per includere una copia di te stesso.

L'apprendimento delle tecniche necessarie da parte dello studente sarebbe ridotto se egli scrivesse un programma che facesse (i) al posto di (ii)? Come si paragonano in quanto a sicurezza? Il programma derivante da (i) potrebbe venire usato da un malfattore per modificare programmi, magari creando dei cavalli di Troia con effetti dannosi ovunque egli decidesse di introdurli. Il programma derivante da (ii) è un virus e, come si è detto, capace di diffondersi indefinitamente, modificando altri programmi con risultati imprevedibili. Per cui: (i) è uno strumento che, se usato con cattive intenzioni, può causare danni -- più o meno come un'ascia; (ii) può diffondersi molto rapidamente partendo da un unico incidente o da una banale disattenzione. Un mozzicone di sigaretta e un'ascia possono entrambi distruggere una foresta, ma in un caso occorre molto più lavoro e determinazione. Perciò nuovi metodi di infezione possono essere esaminati creando programmi in grado di creare altri programmi in

modo arbitrario -- che siano in grado di replicare se stessi non è necessario per capire il meccanismo.

Le università dovrebbero insegnare agli studenti come lavorare e compiere ricerche in maniera sicura e morale. Gli studenti di medicina non si mettono a tagliare persone ancora vive, ma imparano le incisioni anatomiche agendo su dei cadaveri. Quando studiavo microbiologia e ingegneria genetica, ci insegnavano come contenere i nostri esperimenti, come sterilizzare la nostra attrezzatura prima e dopo, e come sistemare in modo sicuro le colture. Gli studenti di informatica dovrebbero imparare ad effettuare ricerche sui virus senza doverli creare.

C'è bisogno di insegnare queste cose, ma ciò non comporta pratiche di scrittura dei virus, così come l'addestramento degli agenti di polizia non comporta pratiche di omicidio. Comprendere il funzionamento di un codice auto-replicante è diverso da scriverlo. Infatti il "reverse engineering" è un'abilità molto più importante per un ricercatore antivirus: quando ti viene presentato un programma sconosciuto, come fai a capire tutto quel che fa, senza permettergli inavvertitamente di causare danni o di sfuggirti di mano?

Spero che questo chiarisca il perché scrivere virus non sia necessario da parte degli studenti, e perché il farlo non sia un atto responsabile. Molti ricercatori antivirus hanno la stessa opinione a riguardo, come si può leggere in questa lettera aperta:

<<http://www.avien.org/publicletter.htm>>

I firmatari non sono soltanto interni ad aziende di antivirus; molti provengono da colossi dell'industria dell'IT, molti sono utenti dell'IT, fra cui organizzazioni accademiche e commerciali. L'Università di Calgary ha una propria libertà accademica, ma dovrebbe meditare sul perché molti dei suoi pari, e molti fra coloro che appartengono al campo che l'università dichiara di servire, stiano avanzando delle obiezioni prima di procedere.

Da: Paul Kocher <paul@cryptography.com>

Oggetto: Attaccare macchine virtuali tramite errori di memoria

Alla fine del suo commento sull'oggetto in questione, lei scrive: "Ora che l'attacco è conosciuto, può essere facilmente prevenuto. Semplici contromisure quali il parity check o codici di correzione degli errori possono sconfiggere questa tecnica".

Questi attacchi basati sulle anomalie sono noti da parecchio (e questo ne è un esempio creativo), e si sono dimostrati estremamente difficili da prevenire. La correzione degli errori può essere d'aiuto, ma spesso non fa altro che costringere l'aggressore a colpire il bersaglio in maniera più dura finché non salta fuori qualche errore. Anche la rilevazione degli errori può essere utile, ma crea un nuovo problema: una ridotta affidabilità. Questi approcci si applicano più facilmente alla RAM, ma non altrettanto si può dire nel caso dei processori, e altre porzioni possono essere avariate.

Infine, anche la considerazione secondo cui il problema sarà risolto perché ora è noto, è ottimistica. Alcuni rivenditori faranno un ottimo lavoro, ma altri ignoreranno del tutto la cosa finché non perderanno clienti a causa del problema.

Da: George Robert Blakley III <blakley@us.ibm.com>

Oggetto: Le monetine durante le partite

Quando ero ragazzo, a Buffalo, ero solito andare a veder giocare la squadra di hockey dei Sabres. Allora non erano un granché, ma avevano di certo dei tifosi perfidi. Quando una squadra avversaria particolarmente malvista (come i Boston Bruins) veniva in città, i tifosi cominciavano a prendere delle monetine, a scaldarle tenendole in mano per un paio di minuti,

e a tirarle nel campo di ghiaccio. Dato che i giocatori indossavano molti rinforzi, caschi, ecc., era piuttosto improbabile che una moneta ferisse un giocatore a causa dell'impatto. Ma non era quello l'obiettivo. Lo scopo era molto più sottile: una moneta calda affonda un poco nel ghiaccio, e a quel punto diventa un ostacolo significativo per i pattini. A volte ci volevano 30-40 minuti per estrarre tutte le monetine dal ghiaccio e ripulire l'intera superficie di gioco.

Da: Owen Minns <Owen@oakspan.com>
Oggetto: DVD che si autodistruggono

Lei suggerisce che tale tecnologia "ha risolto il problema di aver bisogno di un'infrastruttura per gestire i DVD resi". Negli USA, forse, ma a livello globale ciò non solleva la Disney da questa responsabilità. Tale sistema potrà funzionare negli Stati Uniti, dove la Disney e altre compagnie possono ancora convincere i consumatori a comperare prodotti e confezioni costose che diventano spazzatura nel giro di pochi giorni; ma nell'UE il progresso ha imposto ai produttori una responsabilità maggiore per quanto pertiene all'intero ciclo vitale dei loro prodotti, fra cui lo smaltimento degli stessi. Presumibilmente Disney sarà responsabile della gestione e dello smaltimento degli "ex DVD" in quella giurisdizione più ragionevole.

Ci si augura che un'azienda come Disney, con tutte le risorse che ha, si metta a sviluppare misure di sicurezza affidabili senza produrre ancora più rifiuti!

Da: Greg Jennings <gjennings@mail.communica.com>
Oggetto: Comunicare per telefono i dati del proprio account

Il link che lei ha fornito alla vicenda di DirecTV (hacking ai danni della privacy dei clienti in DirecTV) nel numero di Crypto-Gram del 15 giugno, mi ha fatto venire in mente come l'addetto di un negozio e un complice possano ottenere le informazioni relative a una carta di credito.

Una volta mi è capitato di acquistare un oggetto costoso con la mia Visa. Il computer ha apparentemente detto al commesso di chiamare la Visa, e poi mi è stato passato il ricevitore. Il rappresentante della Visa mi ha chiesto conferma del mio numero di telefono e del nome da nubile di mia madre, dopodiché ha permesso alla transazione di proseguire.

Anche se all'epoca non ci ho nemmeno pensato, non avevo modo di verificare che la persona all'altro capo del telefono fosse della Visa! Avrebbe potuto essere facilmente qualcuno nel retro del negozio o in qualsiasi altro luogo, se è per questo.

[Quel che segue è la più strana comunicazione postale che io abbia mai ricevuto, per svariati ordini di grandezza. La trascrivo qui a solo scopo di intrattenimento].

Da: Qualcuno, da qualche parte
Oggetto: [Non ne ho la più pallida idea]

Il 15 gennaio 2003, stavo facendo del banking on-line presso la Lee Bank a Lee, Massachusetts. Zone Alarm mi ha informato sul computer (quasi ogni cosa che possiedo è documentata) che un "presunto hacker" stava cercando di introdursi nel mio conto. Ho trascritto i numeri delle porte, chiamato la banca, e una segretaria molto giovane mi ha detto che avrei dovuto presentarmi e farmi cambiare la password. Ovviamente la Lee Bank si è in seguito rifiutata di procedere, sostenendo che i loro sistemi erano completamente sicuri. Ho pensato "ah, stanno semplicemente cambiando i loro sistemi. Richiamerò fra un quarto d'ora. Mi è stato detto di presentarmi e di farmi cambiare la password. La banca, naturalmente, si è poi rifiutata. I numeri di porte erano gli stessi che avrei incontrato più tardi.

Quindici minuti dopo ero di nuovo al mio terminale e c'era l'e-mail gialla del mio ex-marito (e della sua attuale moglie) in bella evidenza. Stava spedendosi le cose come aveva fatto nel corso degli anni. Aveva ogni sorta di spyware installato sul nostro primo computer. Quando ci eravamo liberati del nostro Windows 95, avevo deciso di comprare a Jake un nuovo computer (ho due figli, Jake e Hallie, e mi sono risposata nel 2000). Il nuovo Compaq fu acquistato nel 1999. Non so per quanto tempo lui si sia spedito le cose indietro. Quando ho premuto "file" mi sono trovata davanti la foto di nostra figlia. Poi ho premuto "source & view" e infine "print". La stampa è partita e hanno cominciato ad uscire un sacco di pagine, talmente tante che è finita la carta. Ho mostrato queste cose ad un esperto di informatica forense a Boston. Ha detto che il programma potrebbe dimostrare che stessero riciclando denaro sporco, che fossero immischiati in pornografia o che Chuck stesse rubando soldi dal conto bancario di George Gilder. George Gilder è la persona responsabile delle previsioni di mercato nel rapporto della Gilder Technology.

La prego di scusare questa lettera molto poco professionale. Casa mia è stata sottoposta ad effrazioni continue, notte dopo notte. Tutti i miei gioielli sono stati scambiati con del filo di rame e numerati. Tutto quello che toccavo sembrava essere un piccolo disco per racchiudere informazioni, ed è stato ricoperto da microchip in argento e rame.

Nessuno mi ha creduto. Ho iniziato di recente a prendere medicine per curare i disturbi da deficit di attenzione, cosa che ha imbestialito il mio secondo marito. Non ne sapevo nulla del fatto che lui poteva essere coinvolto in quel che io credo sia crittografia. Ho trovato una borsa che l'FBI verificherà in cerca di sostanze. Mi sono alzata e mi sono sentita intontita. Ogni giorno sono stata pedinata dalla stessa auto. Volevano sapere quando avrebbero potuto usare casa mia. Un investigatore privato di New York verrà a trovarmi stasera. L'FBI verrà domani. Ho ricevuto una borsa dal New Mexico che ho cercato su Internet. Non mi veniva permesso di usare il computer se non eseguivo il programma del mio ex marito. Le mie chiamate venivano intercettate. Credevamo di avere la DSL di Verizon. Il mio computer veniva controllato dal mio ex marito Edward Charles Frank. Avevo letto nei suoi appunti che stava eseguendo i v2k. Quando mi svegliavo la mattina, c'erano dei floppy disk sul comodino, e dovevo usarli, e non sono un'esperto di informatica forense ma sapevo che non c'erano certo registrati dei versi della bibbia.

Ora viene la parte difficile. Delle persone si sono introdotte in casa mia almeno una decina di volte. Orologi, borse, cappotti, e la mia stessa fiducia in me, sulla mia stessa esistenza, scomparivano e ricomparivano ogni giorno.

La polizia di Lee non è mai venuta a casa mia, neanche una volta. Si sono rivolti a un ospedale psichiatrico: una delle peggiori esperienze che abbia mai affrontato. L'assistente sociale ha detto che i miei problemi sembravano essere legati a cause esterne, e la polizia di stato mi ha tirato fuori, e io so come fare domande in maniera calma ed educata, visto che sono una cantante d'opera. Ma ho smesso di cantare. Avevano già detto loro (credo) che io ero pazza, o forse sono stati pagati. Non riesco a credere al trattamento che ho dovuto subire. Quando li chiamavo per denunciare il furto della mia borsetta, avvenuto in casa mia di notte, mi rispondevano "Oh, dovrà attendere e parlare direttamente con l'agente Buffis, che ha in mano la faccenda". Per settimane sono stata seguita dalle stesse auto. Qualcosa che avevo addosso li informava sulle mie coordinate. Avevano una copia delle chiavi di casa mia e delle mie automobili. Mi hanno cambiato le serrature. Quella notte hanno scassinato persino la serratura della mia camera da letto.

Ho sentito un nastro del mio attuale marito mentre verifica i microfoni, e ho anche scoperto un nastro su cui è incisa la mia voce, mentre parlo distintamente in ogni stanza della casa.

Ci sono molte altre cose da dire in merito a questa storia, e molti misteri da risolvere. Credo di essere nella posizione per chiedere un risarcimento per i vari abusi mentali a cui sono stata sottoposta e per tutto quel che ho sofferto. 3 computer sono da Kroll. Lavorerò insieme a me? Ho cominciato a trascrivere targhe di automobili (circa 7 o 8). Giusto questo pomeriggio, tutte

