



Sei minuti dopo, "parecchie" console di controllo remoto hanno smesso di funzionare. Alle 14:41 si è guastato il server principale adibito alle funzioni di allarme. I suoi servizi sono passati ad un computer di backup, che si è guastato alle 14:54.

Tutto questo non sembra forse un worm che si sta facendo strada attraverso i computer operativi di FirstEnergy?

Secondo il rapporto, "...per più di un'ora nessuno all'interno della sala di controllo di FirstEnergy si è reso conto che le macchine non stavano funzionando correttamente, anche se lo staff tecnico di supporto era al corrente del problema e stava facendo il possibile per risolverlo..."

E tutto questo non suona forse come uno staff tecnico al lavoro per eliminare un worm dal network aziendale?

Questo grave ed esteso malfunzionamento informatico è stato critico nei confronti dell'interruzione di corrente a cascata. Il rapporto prosegue: "Chi opera nelle centrali elettriche conta moltissimo sugli allarmi acustici e a video, e sui log di allarme, per mostrare ogni cambiamento significativo nelle condizioni dei propri sistemi. Dopo le 14:14 EDT del 14 agosto, gli operatori della FE stavano lavorando in una situazione davvero limitata senza questi strumenti. Ed erano esposti ad un pericolo ulteriore, perché non sapevano di lavorare senza allarmi, e non si sono resi conto che le condizioni del sistema stavano cambiando".

Nel rapporto vengono menzionate altre anomalie dei sistemi informatici. Alla Midwest Independent Transmission System Operator, un'agenzia regionale che tiene sotto controllo la distribuzione elettrica, c'è una macchina chiamata "state estimator" [lett. "verificatore di stato"]. Si tratta di un computer utilizzato per determinare se la rete elettrica presenta problemi. Anche questo computer ha smesso di funzionare, alle 12:15. Secondo il rapporto, un tecnico ha tentato di ripararlo ma si è dimenticato di riattivarlo quando si è assentato per pranzo.

Il worm Blaster è apparso per la prima volta l'11 agosto, e ha infettato più di un milione di computer nei giorni successivi. Ha preso di mira una vulnerabilità nel sistema operativo Microsoft. I computer infettati hanno a loro volta cercato di colpire altri computer, e in questo modo il worm si è propagato automaticamente da computer a computer e da network a network. Anche se il worm non eseguiva alcuna azione maligna nei computer infettati, la sua mera esistenza attingeva a tal punto dalle risorse del sistema da mandare il computer in crash. Per rimuovere il worm un amministratore di sistema doveva lanciare un programma per cancellare il codice maligno; poi doveva applicare una patch alla vulnerabilità per evitare che il computer fosse nuovamente colpito.

Secondo una ricerca di Stuart Staniford, Blaster era uno scanner sequenziale a indirizzo di partenza casuale, e la sua velocità di scansione era di 11 IP al secondo. Un tale scanner coprirebbe un network di classe B in circa un'ora e 40 minuti. Gli orari delle anomalie ai computer della FirstEnergy presentano forti analogie con la tipica situazione di una rete di computer, tutti con indirizzi di classe B, che viene compromessa da uno scan della classe B, forse da una macchina infetta sulla stessa rete. (Si noti che non era necessario che il network di FirstEnergy fosse in Internet; Blaster ha infettato molte sottoreti interne).

La coincidenza dei tempi è troppo ovvia per essere ignorata. Alle 14:14 EDT, il worm Blaster stava facendo fuori svariati sistemi lungo tutto il nordamerica. Il rapporto non spiega perché così tanti computer -- sia sistemi primari, sia di backup -- alla FirstEnergy presentavano malfunzionamenti intorno agli stessi orari, ma Blaster è di certo un ragionevole sospettato.

Purtroppo il rapporto non fa riferimenti diretti al worm Blaster e ai suoi effetti sui computer della FirstEnergy. Il massimo che sono riuscito a trovare è il periodo seguente, a pagina 99: "Malgrado un discreto numero di worm e virus fosse in azione su Internet e sui sistemi e i

network connessi ad Internet nel nordamerica prima e durante il black-out, le analisi preliminari di SWG non indicano che tale attività di worm e virus abbiano avuto un impatto significativo sui sistemi di generazione e distribuzione della corrente elettrica. Successive analisi di SWG verificheranno questo accertamento”.

Perché tutta questa prosa intricata? Gli autori ce la mettono tutta per assicurarci che “i sistemi di generazione e distribuzione della corrente elettrica” non sono stati colpiti da Blaster. E i sistemi di allarme? È evidente che sono stati tutti attaccati da qualcosa, tutti nello stesso momento.

Questa non sarebbe la prima volta che un agente epidemico in Windows si introduce nella rete di FirstEnergy. L'azienda ha ammesso di essere stata colpita da Slammer a gennaio.

Siamo onesti. Non so se Blaster ha causato il black-out. Il rapporto non dice che Blaster ha causato il black-out. L'opinione prevalente è che Blaster non ha causato il black-out, ma pare sempre più probabile che Blaster è stata una delle molte cause del black-out.

A prescindere dalla risposta, qui c'è una morale molto importante. Mentre dei computer collegati in rete vanno ad inserirsi sempre più all'interno della nostra infrastruttura critica, tale infrastruttura diventa vulnerabile non solo agli attacchi, ma anche a software e ad operazioni approssimative. Queste vulnerabilità finiscono sempre col non essere le più ovvie. I computer che controllano direttamente la rete elettrica sono ben protetti, ma sono i sistemi periferici a non essere così al sicuro e più soggetti a vulnerabilità. E un attacco diretto difficilmente procurerà danni alla nostra infrastruttura, poiché le connessioni sono troppo complesse e troppo oscure. Questi gravi malfunzionamenti su larga scala avvengono solo incidentalmente, per esempio grazie a un worm come Blaster che infetta i sistemi proprio nel momento sbagliato, facendo sì che un minimo guasto assuma proporzioni smisurate.

Abbiamo visto worm mettere fuori uso il servizio telefonico di emergenza 911. Abbiamo visto worm disattivare i bancomat. Niente di tutto questo era prevedibile, ma può essere impedito. Credo che cose di questo genere sono destinate a diventare sempre più comuni in futuro.

Una versione preliminare di questo articolo è apparsa su news.com:

<<http://news.com.com/2010-7343-5117862.html>>

“Interim Report: Causes of the August 14th Blackout in the United States and Canada.”

<<https://reports.energy.gov/814BlackoutReport.pdf>>

I dati più rilevanti sono alle pagine 28 e 29 del rapporto.

FirstEnergy fu colpita da Slammer:

<<http://www.securityfocus.com/news/6868>>

<<http://www.computerworld.com/securitytopics/security/recovery/story/0,10801,84203,00.html>> oppure <<http://tinyurl.com/z9to>>

Come i worm possono infettare reti interne:

<<http://www.networm.org/faq/#enterprise>>

Il black-out non è stato causato da worm:

<[http://news.com.com/2100-7355\\_3-5111816.html](http://news.com.com/2100-7355_3-5111816.html)>

Un articolo di news sul rapporto:

<<http://www.iht.com/articles/118457.html>>



<[http://www.nbr.co.nz/home/column\\_article.asp?id=7586&cid=3&cname=Technology](http://www.nbr.co.nz/home/column_article.asp?id=7586&cid=3&cname=Technology)> oppure <<http://tinyurl.com/z9tq>>  
<<http://www.theregister.co.uk/content/68/34096.html>>  
<<http://star-techcentral.com/tech/story.asp?file=/2003/11/19/technology/6747626&sec=technology>> oppure <<http://tinyurl.com/z9tr>>  
<<http://economictimes.indiatimes.com/cms.dll/articleshow?msid=290188>>

Raseac è un'altra azienda che realizza telefoni con crittografia:  
<<http://www.raseac.com.br/>>

\*\* \*\*

Il Canile: Amit Yoran

Cominciamo con una domanda: se non credete sia possibile migliorare la sicurezza del codice, che ci state a fare nell'industria della sicurezza informatica?

"Amit Yoran, il nuovo capo della divisione cyber-sicurezza del Dipartimento della Sicurezza Nazionale, ha affermato che l'amministrazione sta valutando l'impatto di alcune proposte regolatrici in questo ambito. Una di queste richiederebbe alle aziende di comunicare, attraverso la Commissione di Controllo della borsa, il loro grado di preparazione nei confronti di eventuali attacchi alle proprie reti informatiche. Mr. Yoran, in precedenza un vicepresidente della Symantec Corp., ha detto che il dipartimento sta considerando altre misure, anche se la tendenza è rivolta ad approcci al settore privato".

"Per esempio, dovremmo ritenere i produttori di software responsabili della sicurezza del loro codice o per quanto concerne eventuali falle nel loro codice?" si è chiesto Yoran durante un'intervista. "In teoria, ciò può avere un senso. Ma in pratica, sono in possesso delle capacità e degli strumenti per produrre un codice più sicuro?".

Sono esterrefatto dalla totale idiozia di questo estratto. Ma pensa davvero che scrivere codice più sicuro è qualcosa di troppo difficile da gestire per quelle aziende? Pensa davvero che le compagnie stanno facendo assolutamente il meglio che possono?

Riesco a tollerare un certo livello di compiacenza verso l'industria, ma tutto questo è troppo stupido per essere ignorato.

L'articolo:  
<<http://online.wsj.com/article/0,,SB107040249488089600,00.html>>  
<<http://news.com.com/2008-7355-5112350.html>>

\*\* \*\*

Le ristampe di Crypto-Gram

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

Il contrattacco  
<<http://www.schneier.com./crypto-gram-0212.html#1>> (originale)  
<<http://www.crypto-gram.it/dicembre02.htm#a1>> (traduzione)

Osservazioni sul Dipartimento per la Sicurezza Nazionale  
<<http://www.schneier.com./crypto-gram-0212.html#3>>  
<<http://www.crypto-gram.it/dicembre02.htm#a3>>

Il crimine, ovvero la prossima grande novità di Internet  
<<http://www.schneier.com./crypto-gram-0212.html#7>>  
<<http://www.crypto-gram.it/dicembre02.htm#a7>>

Documenti d'identità nazionali:  
<<http://www.schneier.com/crypto-gram-0112.html#1>>  
<<http://www.crypto-gram.it/dicembre.html#a1>>

I giudici puniscono le pessime misure di sicurezza:  
<<http://www.schneier.com/crypto-gram-0112.html#2>>  
<<http://www.crypto-gram.it/dicembre.html#a2>>

Sicurezza informatica e responsabilità:  
<<http://www.schneier.com/crypto-gram-0112.html#4>>  
<<http://www.crypto-gram.it/dicembre.html#a4>>

Farsi beffe degli scanner di vulnerabilità:  
<<http://www.schneier.com/crypto-gram-0112.html#9>>  
<<http://www.crypto-gram.it/dicembre.html#a9>>

Le votazioni e la tecnologia:  
<<http://www.schneier.com/crypto-gram-0012.html#1>>

“La sicurezza non è un prodotto; è un processo”:  
<<http://www.schneier.com/crypto-gram-9912.html#1>>

La tecnologia Echelon:  
<<http://www.schneier.com/crypto-gram-9912.html#3>>

Gli algoritmi digitali cellulari europei:  
<<http://www.schneier.com/crypto-gram-9912.html#10>>

L'inutilità delle gare di cracking:  
<<http://www.schneier.com/crypto-gram-9812.html#contests>>

Come riconoscere il testo in chiaro (plaintext):  
<<http://www.schneier.com/crypto-gram-9812.html#plaintext>>

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

## Crittografia quantica

MagiQ Technologies sta vendendo un vero e proprio prodotto che fa uso di singoli fotoni per scambiare chiavi su linee a fibre ottiche. I sistemi Navajo sfruttano i fotoni per trasmettere chiavi crittografiche su linee a fibre ottiche e la sicurezza si basa sulla legge dei quanti secondo cui un osservatore (chi intercetta, in questo caso) perturba un sistema osservandolo.

Non è nulla di nuovo. La scienza nelle sue linee base è stata sviluppata nei primi anni Ottanta, e sono stati fatti grandi progressi ingegneristici da allora. Nella seconda edizione di “Applied Cryptography” (alle pagine 554-557) descrivo in sintesi come funziona tutto questo processo.





Vi sono decine di storie riguardanti macchine per il voto elettronico che producono risultati sbagliati. Voti che appaiono o scompaiono misteriosamente. Voti indirizzati a una persona e accreditati ad un'altra. Ecco due episodi dalle elezioni più recenti: un candidato in Virginia ha scoperto che le macchine per il voto elettronico sbagliavano nel registrare i suoi voti, e infatti tendevano a sottrarre un voto a suo favore circa ogni cento voti. E nell'Indiana, 5.352 votanti in un distretto di 19.000 sono riusciti a registrare 144.000 voti su una macchina per il voto elettronico.

Questi problemi sono stati rilevati solamente perché hanno prodotto delle conseguenze visibili, e visibilmente erranee. Problemi meno vistosi continuano a sfuggire, e per ogni caso scoperto (anche se spesso non è possibile annullare gli sbagli) ve ne sono probabilmente decine che passano inosservati.

I computer sono fallibili e il software inaffidabile; le macchine utilizzate per le elezioni non sono diverse dal computer che avete in casa.

La cosa ancor più preoccupante degli errori del software è il potenziale per un'eventuale frode. Le aziende che producono il software delle macchine per il voto elettronico non si servono di adeguate pratiche per la sicurezza informatica. Molto del codice sensibile viene lasciato senza protezione sulle reti aziendali. Installano patch e aggiornamenti senza un adeguato auditing di sicurezza. E si servono della legge per proibire una verifica pubblica delle loro pratiche. Quando alla Diebold divennero pubbliche alcune annotazioni compromettenti, la compagnia fece scattare denunce al fine di eliminarle. Con queste pratiche di sicurezza informatica così approssimative, come possiamo essere sicuri che nessuno si sia infiltrato nella rete aziendale e abbia modificato il software per il voto?

E dato che le elezioni sono un evento estremamente immediato e avvengono in contemporanea, non ci sarebbero possibilità di rimediare al problema. Supponiamo che alle prossime elezioni presidenziali qualcuno modifichi il voto di New York. Si farà votare di nuovo la città di New York dopo una settimana? Si rifaranno completamente le elezioni nazionali? Si dirà ai cittadini di New York che i loro voti non contano?

Ogni dibattito sul voto elettronico porta necessariamente al discorso del voto via internet. Perché non eliminare del tutto le macchine per il voto elettronico e lasciare che la gente voti in remoto?

I sistemi di voto online presentano un potenziale di errore e di abuso ancora più alto. I sistemi via internet sono estremamente difficili da proteggere, come si può vedere dalla scia infinita di vulnerabilità informatiche e dall'effetto a macchia d'olio di worm e virus. Certo, sarebbe comodo poter votare dal proprio computer a casa, ma questo darebbe nuove opportunità a certa gente di giocare a Trucca il Voto.

E qualsiasi sistema di voto remoto ha i propri inconvenienti. La cabina elettorale offre sicurezza contro la coercizione. Io posso venire corrotto o minacciato per votare in un certo modo, ma quando entro nella privacy della cabina elettorale posso votare come mi pare. Il voto remoto, sia per posta o via internet, non offre questa sicurezza. La persona che compra il mio voto può avere la certezza di comprarlo prendendo la mia scheda vuota e compilandola al mio posto.

Negli Stati Uniti crediamo che permettere agli assenti di votare sia più importante di questa sicurezza aggiuntiva, e che sia probabilmente un buon compromesso. E alla gente piace questa comodità: in California, per esempio, più del 25% degli elettori vota per posta.

Votare, negli Stati Uniti, è particolarmente difficile per due motivi. Primo, si vota su decine di cose diverse in una volta sola. Secondo, si pretende di avere i risultati finali entro il giorno stesso della votazione.

Ciò di cui abbiamo bisogno sono sistemi di voto molto semplici: schede di carta che possono essere contate anche in caso di black-out. Abbiamo bisogno della tecnologia per semplificare il procedimento di voto, ma questa deve essere affidabile e verificabile.

Quel che suggerisco è semplice, ed è la stessa cosa che consigliano molti altri ricercatori della sicurezza informatica. Tutte le macchine per il voto elettronico devono essere dotate di una traccia di controllo cartacea. Costruite il macchinario elettronico che volete, fate in modo che funzioni come volete. L'elettore esprime il suo voto, e quando ha finito la macchina stampa una ricevuta, come fanno i bancomat. La ricevuta è la scheda di voto vera e propria. L'elettore la controlla e poi la lascia in un apposito contenitore. Tale scatola conterrà i voti ufficiali, che saranno usati per qualsiasi verifica. Alla macchina per il voto è lasciato un primo veloce riscontro.

Questo sistema non è perfetto, e non risolve molte problematiche di sicurezza intorno al sistema di voto. È ancora possibile negare alle persone il diritto di voto, o riempire macchine e contenitori con falsi voti, perdere macchine e scatole con le schede, minacciare gli elettori, ecc. Le macchine computerizzate non rendono il voto completamente sicuro, ma dispositivi con una traccia di controllo cartacea possono prevenire nuovi tipi di errore e tentativi di frode.

Il rapporto del CRS sul Voto Elettronico:

<<http://www.epic.org/privacy/voting/crsreport.pdf>>

Alcune risorse sul voto elettronico:

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

<<http://www.eff.org/Activism/E-voting/>>

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

<<http://electioncentral.blog-city.com/index.cfm>>

Proposte di legge del governo americano per rendere obbligatorio un controllo sul voto:

<<http://graham.senate.gov/pr120903.html>>

<<http://holt.house.gov/issues2.cfm?id=5996>>

L'episodio accaduto in Virginia:

<<http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A6291-2003Nov5>> oppure <<http://tinyurl.com/z9uc>>

L'episodio accaduto nell'Indiana:

<<http://www.indystar.com/articles/1/089939-1241-014.html>>

L'episodio accaduto in Nevada:

<<http://www.lasvegassun.com/sunbin/stories/lv-gov/2003/dec/10/515999082.html>>

oppure <<http://tinyurl.com/z9ud>>

Dichiarazione del Segretario di Stato della California sui requisiti per una traccia di controllo cartacea nel voto elettronico:

<[http://www.ss.ca.gov/executive/press\\_releases/2003/03\\_106.pdf](http://www.ss.ca.gov/executive/press_releases/2003/03_106.pdf)>

L'episodio accaduto nel Maryland:

<<http://www.gazette.net/200350/montgomerycty/state/191617-1.html>>

Altre opinioni:

<<http://www.pbs.org/cringely/pulpit/pulpit20031204.html>>

<<http://www.securityfocus.com/columnists/198>>

<<http://www.sacbee.com/content/opinion/story/7837475p-8778055c.html>>



biglietto regolarmente pagato. Non è stato una minaccia per niente e per nessuno. Gli oggetti da lui introdotti non erano neanche particolarmente pericolosi.

Ci si sente violati, se qualcuno penetra in casa nostra, ma soltanto perché lo ha fatto senza permesso. Se un vostro ospite portasse una bistecca in casa vostra durante una cena a base di pesce, la cosa non sarebbe più di tanto seccante.

Non sto dicendo che è stata una mossa geniale, ma quel tipo di violazione non è molto grave, e dovrebbe essere trattata come un reato minore, come lei appunto suggerisce. La TSA dovrebbe smetterla con tutte queste regole di facciata, perché è proprio grazie a queste regole che Heatwole, come lei faceva notare, rischia una condanna penale.

Così un ragazzo che paga il suo biglietto aereo, non crea nessuna reale minaccia, e viola una stupida regola dovrebbe essere severamente perseguito in quanto "hacker"? La legge dovrebbe essere fatta per proteggere e non per infastidire, per cui speriamo che quel ragazzo non sia punito con eccessiva severità.

Da: Doug Greene <[gwiz@eTransforms.com](mailto:gwiz@eTransforms.com)>

Oggetto: Gli hacker degli aerei

La sua analogia non è corretta, nella misura in cui il trasporto aereo viene regolato nell'interesse pubblico e la sicurezza è responsabilità del governo. Quindi deve essere soggetta a pubblica supervisione. Non è la stessa situazione di una dimora privata. Chi si sente violato e in imbarazzo qui, se non l'agenzia governativa accusata di non essere in grado di assicurare quel livello di sicurezza che dice di garantire?

Anche lei lo riconosce: "Molto di quel che la TSA svolge è una messinscena, un qualcosa che dia l'idea di sicurezza. Mantiene le apparenze, e forse (si spera) fa in modo che eventuali terroristi non siano così tanto sicuri di poter introdurre armi a bordo di un aereo. Probabilmente no". In ogni caso chi si serve dei servizi di trasporto aereo viene quotidianamente infastidito nel nome di una sicurezza che non funziona. O si fa in modo che funzioni ragionevolmente bene, oppure tanto vale ripristinare le libertà civili che sono state infrante in nome di questi sistemi di sicurezza quantomeno disonesti.

Lei dice: "la TSA non gli ha mai chiesto di collaudare tale sicurezza". Certo che no. È assai più probabile che chi viene incaricato dalla TSA di collaudare la sicurezza tenderà a mantenerne nascoste le falle agli occhi dell'opinione pubblica.

Occorrono leggi che permettano un certo tipo di verifiche indipendenti su questi sistemi di sicurezza, nel pubblico interesse. In questo modo, bravate come quella di Nathaniel Heatwole sono di certo migliori che non delle verifiche interessate e di parte che possono essere state organizzate dalla TSA e non certo nel pubblico interesse.

Da: Brian T. Sniffen <[bts@alum.mit.edu](mailto:bts@alum.mit.edu)>

Oggetto: Gli hacker degli aerei

Credo che lei abbia commesso un grave errore nel suo articolo su Heatwole. Vi sono due punti che lei non ha preso in considerazione, ciascuno dei quali porta a conclusioni molto diverse da quelle da lei delineate.

In primo luogo, esiste un problema di messa a fuoco: i cosiddetti hacker che penetrano in case o computer altrui compiono certamente un atto criminoso. Ma dov'è la differenza fra questo e il

violare l'altrui proprietà intellettuale? Dovremmo forse processare il prossimo ricercatore che scopre falle di sicurezza in un software coperto da copyright? Di certo l'azienda si sentirebbe violata. Ma quando Matt Blaze pubblicò degli scritti che spiegavano quanto insicure fossero le serrature di casa mia, non l'ho considerato un criminale: l'ho ringraziato. E anche lei lo ringraziò, se ben ricordo. Allo stesso tempo Schlage e moltissimi fabbri sparsi per tutto il paese reclamavano a gran voce la sua testa.

In secondo luogo, esiste il problema della responsabilità sociale. C'è differenza fra il penetrare in casa di qualcuno e dimostrare la presenza di una falla in un sistema di sicurezza pubblico che si pone come difensore della pubblica incolumità. Da quel che ho capito del gesto di Heatwole, egli non ha commesso alcun reato: ha seguito le normali procedure di imbarco della TSA, rispettando le regole da loro imposte. Ciò è ben diverso dal forzare una serratura per introdursi in un'abitazione privata o per aggirare dei controlli di sicurezza (sia a livello di software, sia a livello sociale). Considero le azioni di Heatwole come appartenenti alla stessa categoria di quelle commesse da chi ha violato il DMCA e altre leggi sul copyright per mostrare le vulnerabilità nelle macchine Diebold per il voto elettronico: esporre le menzogne o l'incompetenza di chi custodisce la fiducia del pubblico sarà anche in violazione delle leggi, ma dovrebbe essere raramente considerato un reato.

Da: Michael Giagnocavo <[mgg@Atrevido.net](mailto:mgg@Atrevido.net)>

Oggetto: Gli hacker degli aerei

L'effetto sorpresa è stato un exploit su una falla di sicurezza conosciuta: l'accesso alla cabina di pilotaggio. Non mi è possibile toccare alcun controllo quando salgo su un taxi da 5000 dollari, ma alcune persone sono riuscite a penetrare facilmente nella cabina di pilotaggio di un aereo da molti milioni di dollari.

Come nel caso dei buffer overflow (e delle tecniche di mitigation che possono attuare i compilatori), eliminare la sorpresa rende semplicemente più arduo exploitare la falla conosciuta. Il fattore sorpresa è stato solo il loro "codice di exploit" in quell'occasione e per quella falla di sicurezza.

Se assumiamo che quella falla non sia stata ancora chiusa (e l'accesso alla cabina di pilotaggio non sia sprangato), che cosa potrebbe fermare qualcuno dall'asfissiare i passeggeri con un lacrimogeno e prendere nuovamente il controllo dell'aereo?

Da: Ben Mord <[bmord@iconnicholson.com](mailto:bmord@iconnicholson.com)>

Oggetto: Gli hacker degli aerei

Malgrado il suo augurio che in futuro i passeggeri si uniscano contro azioni terroristiche, temo che i nostri aerei rimangano vulnerabili ad azioni di ingegneria sociale. Le lascio questo link come prova:

<[http://cspanrm.fplive.net:554/ramgen/cspan/ldrive/ter082102\\_aviation2.rm](http://cspanrm.fplive.net:554/ramgen/cspan/ldrive/ter082102_aviation2.rm)>

[Nota: si tratta di un filmato in streaming video di due ore e mezza].

Un individuo fuori di sé si è introdotto in una cabina di pilotaggio superandone l'accesso "blindato"; questo in un mondo post-11 settembre, mentre alcune hostess gli stavano offrendo dell'acqua. Grazie al cielo non è accaduto nulla di grave (non è stato il caso di chi utilizzi la propria incoscienza per compromettere la sicurezza della cabina di pilotaggio mentre altri complici aspettano in silenzio il momento di lanciare un secondo attacco). Serva di lezione anche il fatto che questo individuo, pur essendo una persona qualunque e senza alcuna

