

si possono utilizzare per rendere il tutto più semplice da risolvere (questa è un'estrema semplificazione dello studio, ed è consigliabile leggerlo per avere maggiori dettagli).

L'attacco dipende in maniera molto più cruciale dalla complessità delle componenti non lineari, più che dal numero di round. Algoritmi con piccole S-box e strutture semplici sono particolarmente vulnerabili. Serpent possiede piccole S-box e una struttura semplice. AES possiede S-box più grandi, ma una descrizione algebrica molto semplice (anche Twofish possiede piccole S-box, ma una struttura non lineare molto più complessa. Nessuno ha ancora implementato un attacco contro Twofish, ma mi guardo bene dal dichiarare l'algoritmo immune).

Questi sono risultati impressionanti. In passato, gli attacchi migliori funzionavano violando varianti semplificate di AES mediante modelli di attacco assai poco pratici (che richiedono, ad esempio, enormi quantità di testo in chiaro selezionato). Questo studio ha affermato di poter violare l'intero algoritmo, e con solo uno o due testi in chiaro conosciuti. Ma soprattutto il primo algoritmo ad essere violato è stato Serpent, universalmente considerato come la scelta più sicura e conservatrice.

In ambiente accademico c'è stato un po' di movimento riguardo a questo studio, ma le acque si sono calmate presto. Credo che il problema fosse dovuto al fatto che lo studio è denso e difficile da seguire. La tecnica di attacco, chiamata XSL, era completamente nuova (è basata su un'altra tecnica, chiamata XL, presentata all'Eurocrypt 2000). I risultati sono stati così sorprendenti -- un attacco contro Serpent! -- al punto di essere tenuti in poco conto.

Frattanto, Fuller e Millan rilasciavano uno studio che dimostrava come la S-box di 8x8 bit di AES sia in realtà di 8x1 bit: esiste soltanto un'unica parte non lineare all'interno del cifrato, tutto il resto è lineare. Un altro studio arrivava da Filiol, dove egli dichiarava di aver rilevato alcune distorsioni nelle funzioni booleane di AES, che potevano essere potenzialmente usate contro AES. Ma non è possibile dire quanto sia fondata questa dichiarazione, in quanto vi sono ancora troppi pochi dettagli nello studio.

Murphy e Robshaw, a Crypto 2002, hanno pubblicato un risultato sorprendente, che permette all'intero AES di essere espresso in un unico campo. Hanno postulato un cifrato chiamato BES, che tratta ogni byte di AES come un vettore a 8 byte. BES opera su blocchi di 128 byte; per uno speciale sottoinsieme dei testi in chiaro e delle chiavi, BES è isomorfo ad AES. Questa rappresentazione possiede diverse proprietà interessanti che possono renderla più facile da crittoanalizzare.

In maniera ancora più interessante, la rappresentazione BES offre al metodo XSL una rappresentazione molto più concisa, e di conseguenza equazioni meno dense e più semplici da risolvere. In più, vi sono delle versioni intermedie di BES -- vettori a 2 byte, a 4 byte, ecc. -- che diminuiscono in complessità man mano che ci si avvicina a BES-8. Queste rappresentazioni hanno identificato un gruppo ulteriore di equazioni quadratiche che si applicano ad AES e BES. Quando le si butta nel calderone di XSL, l'attacco di Courtois e Pieprzyk viene ad avere una complessità di 2^{100} , di contro alla complessità di 2^{200} , più o meno, dichiarata in precedenza.

Per cui, ecco l'attuale segnapunti. Courtois e Pieprzyk dichiarano un attacco dell'ordine di 2^{100} contro AES, e dell'ordine di 2^{200} contro Serpent. E questa è una cosa seria.

Sempre che sia reale.

Viviamo in un'epoca di crittoanalisi completamente teorica. Le lunghezze delle chiavi dei cifrati sono arrivate a grandezze tali che gli attacchi non possono praticamente essere implementati: la loro complessità è semplicemente troppo alta. Ma l'implementazione è fondamentale; alcuni attacchi manifestano problemi nascosti quando li si prova, e altri si rivelano più efficaci del previsto. Si possono testare gli attacchi su versioni semplificate dell'algoritmo -- meno round,

dimensioni più ridotte dei blocchi -- ma non si è mai certi che un attacco abbia l'effetto previsto. La crittoanalisi differenziale è stata sviluppata in questo modo: l'attacco fu dimostrato su varianti più semplici di DES e poi estrapolato sul DES completo (non credo che l'attacco sia mai stato implementato sul DES completo). Molti degli attacchi che utilizziamo per decifrare algoritmi -- lineare, boomerang, slide, mod n, ecc. -- sono più spesso questioni matematiche che dimostrazioni pratiche. Non credo che nell'arco della nostra esistenza sapremo se l'attacco 2^{100} ai danni di AES funzioni o meno. Abbiamo bisogno di molta più analisi e di verifiche sulla tecnica XSL generale, su algoritmi più deboli e versioni semplificate di veri algoritmi.

Per cui siamo nel pieno del dilemma. Potremmo avere per le mani una strabiliante nuova tecnica crittoanalitica, ma non sappiamo se vi siano errori nell'analisi, e non c'è modo di testare la tecnica per via sperimentale. Occorre aspettare finché altre persone affronteranno lo stesso lavoro. E, per essere sicuri, occorre aspettare finché qualcuno non migliori l'attacco fino a renderlo pratico, prima di sapere se l'algoritmo è stato violato, tanto per cominciare.

Ad ogni modo, non è ancora il caso di allarmarsi. Questi attacchi non possono essere implementati sul campo più di quanto non vengano testati in un laboratorio. Nessun traffico AES (o Serpent) può essere decifrato usando queste tecniche. Nessun genere di comunicazione è a rischio. Nessun prodotto necessita di essere ritirato. Esiste un tale margine di sicurezza in questi cifrati che gli attacchi sono irrilevanti.

Ma c'è ragione di preoccuparsi. Se l'attacco dovesse funzionare davvero, le cose non farebbero altro che peggiorare. Ciò che temo è che si possano avere ottimizzazioni dell'attacco XSL che decifrano AES a un grado di complessità dell'ordine di 2^{80} , nel qual caso le cose diventerebbero pericolose nel giro di dieci anni. Questo è il problema con la crittoanalisi teorica: si sa quando un attacco funziona nello stesso momento in cui si è già in una situazione a rischio.

Il lavoro è affascinante. Durante l'elaborazione di AES, tutti erano d'accordo che Rijndael fosse la scelta rischiosa, e Serpent quella conservatrice, e che Twofish stava a metà strada. Che Serpent fosse il primo a cadere (anche se marginalmente) e che Rijndael dovesse cadere così rapidamente, per ora, sono cose che nessuno aveva previsto. Ma questa è la crittografia. La comunità sviluppa una serie di algoritmi per i quali non esistono attacchi conosciuti, e poi nuovi strumenti di attacco saltano fuori dal nulla e vanno a colpire alcuni di quegli algoritmi. Ci affanniamo tutti, e poi il ciclo si ripete.

Stiamo iniziando a vedere i nuovi strumenti di attacco che funzionano contro alcuni dei finalisti di AES. Per quanto rimarranno strumenti solo teorici è una questione aperta. Ma molti crittografi che prima si erano dimostrati positivi nei confronti di AES, ora cominciano ad avere dei dubbi.

Riassunto dei recenti risultati AES:

<<http://www.cryptosystem.net/aes/>>

Versione preliminare dello studio di Courtois e Pieprzyk (la stesura finale sarà presentata ad Asiacrypt 2002):

<<http://eprint.iacr.org/2002/044/>>

Lo studio di Fuller e Millan:

<<http://eprint.iacr.org/2002/111/>>

Il contributo di Filiol:

<<http://eprint.iacr.org/2002/099/>>

Lo studio di Murphy e Robshaw:

<<http://www.isg.rhul.ac.uk/~mrobshaw/aes-crypto.pdf>>

Testo di una canzone: "Bit Commitment Blues" (il blues del bit imprigionato):
<<http://home.datawest.net/staym/commit.html>>

Un buon articolo su tutto il sensazionalismo e le idiozie riguardanti cyber-guerre e cyber-terrorismo:
<<http://www.zdnet.it/zdnet/JumpNews.asp?idNews=150295>>

Uno scritto sui rischi connessi al trasferimento della Computer Security Division del NIST al Dipartimento per la Sicurezza Nazionale:
<http://www.boston.com/dailyglobe2/230/business/Cybersecurity_should_be_kept_in_civilian_hands+.shtml>
<<http://makeashorterlink.com/?S5DF257C1>>

Possibili brevetti di Palladium da parte di Microsoft:
6,330,670 Sistema operativo di gestione dei diritti digitali
6,327,652 Caricamento e identificazione di un sistema operativo di gestione dei diritti digitali

Ve ne saranno probabilmente molti altri in attesa di brevetto in Europa, dove occorre rivelare informazioni all'atto di presentazione dell'istanza.

Ad una tavola rotonda su Palladium alla USENIX Security Conference in agosto, i rappresentanti di Microsoft hanno dichiarato che Palladium non poteva essere usato in alcun modo per far rispettare il Digital Rights Management. In risposta Lucky Green ha trovato una serie di modalità con le quali Palladium poteva invece essere usato allo scopo e poi far richiesta formale di brevetto.

<<http://www.mail-archive.com/cryptography@wasabisystems.com/msg02506.html>>
<<http://www.mail-archive.com/cryptography@wasabisystems.com/msg02554.html>>

Eccellente articolo sul sabotaggio dei tavoli di blackjack a Las Vegas. Pare che se da un lato a Las Vegas sapevano come scoprire i contatori di carte, dall'altro non potevano rilevare contatori che lavoravano in squadra.
<http://www.wired.com/wired/archive/10.09/vegas_pr.html>

Una nuova compagnia, la PGP Corp., ha acquistato PGP da Network Associates:
<<http://www.zdnet.it/zdnet/JumpNews.asp?idChannel=917&idNews=150299>>

Gli hacker vogliono che le persone noiose la smettano di criptare tutto:
<<http://www.satirewire.com/news/aug02/encryption.shtml>>

Leggete questa notizia per i commenti alla fine, dove un ufficiale dell'intelligence britannica, di fronte all'evidenza che i suoi segreti sono stati intercettati, suggerisce che il governo dovrebbe bandire gli scanner. Probabilmente pensa che così facendo sarebbe più facile che non risolvere il problema.
<<http://news.bbc.co.uk/1/hi/uk/2065342.stm>>

Un buon articolo sui rischi realistici del cyber-terrorismo:
<<http://zdnet.com.com/2100-1105-955293.html>>

C'è una nuova libreria in C per Twofish, scritta da Niels Ferguson. Le differenze principali rispetto al codice esistente è che questa è completamente portabile, facile da integrare, ben documentata; inoltre contiene una serie approfondita di auto-test. Ed è totalmente gratuita.
<<http://niels.ferguson.net/code/TwofishClib.html>>

Le libertà civili dopo l'11 settembre; la cronologia di EPIC:
<<http://www.epic.org/default91102.html>>

"Non ne vado per niente fiero", ha dichiarato Brian Valentine (vice presidente senior del team di sviluppo di Microsoft Windows) davanti a una folla di sviluppatori alla conferenza per lo sviluppo di Windows .Net Server. "Non abbiamo proprio fatto tutto quel che si poteva fare per proteggere i nostri clienti... I nostri prodotti non sono affatto costruiti per la sicurezza".
<<http://staging.infoworld.com/articles/hn/xml/02/09/05/020905hnmssecure.xml>>

Craig Mundie, di Microsoft, sulla sicurezza. La mia frase preferita: "La gente confonde la 'sicurezza' e il Trustworthy Computing".
<<http://www.microsoft.com/PressPass/features/2002/feb02/02-20mundieqa.asp>>

La RIAA denuncia Verizon; entrambe le parti si rifanno al DMCA:
<<http://www.washingtonpost.com/wp-dyn/articles/A38034-2002Sep4.html>>

Buon materiale riguardante le votazioni elettroniche:
<<http://www.notablessoftware.com/RMstatement.html>>
<<http://www.notablessoftware.com/checklists.html>>

Di recente ho sentito voci che mi danno favorevole al voto elettronico, alle votazioni via Internet, eccetera. Questo non potrebbe essere più lontano dal vero. Ecco la mia posizione:
<<http://www.counterpane.com/crypto-gram-0102.html#10>>
<<http://www.counterpane.com/crypto-gram-0012.html#1>>

** ** ** * * * * *

Le news di Counterpane

Schneier interverrà a Seattle, Vancouver, Columbus e Sacramento, per parlare del lavoro di Counterpane per il monitoraggio. Per maggiori informazioni:
<<http://www.counterpane.com/conf.html>>

Schneier terrà un keynote in occasione dell'ISSE 2002, a Disneyland, Parigi, il 2 ottobre.
<<http://www.isse.org/>>

Schneier interverrà allo SMAU 2002 a Milano il 25 ottobre.
<<http://www.smau.it/smau2002/english/docs/flash.html>>

Schneier interverrà e farà parte di una tavola rotonda al Symposium sulla Privacy e sulla Sicurezza a Zurigo, Svizzera, il 30-31 ottobre.
<<http://www.privacy-security.ch>>

** ** ** * * * * *

Una vulnerabilità di Microsoft Word 97

Ecco la vulnerabilità. Alice manda a Bob un documento Word. Bob lo corregge e glielo rimanda. All'insaputa di Bob, il documento che lui rispedisce può contenere qualsiasi file del suo computer. Tutto ciò che ad Alice occorre sapere è il pathname del file.

Per sfruttare questa vulnerabilità, Alice incorpora un codice particolare nel documento Word che manda a Bob. Quando Bob apre il documento, Word prende il file e lo incorpora nel documento. Bob non vede che cosa sta succedendo, e non ha modo di saperlo. Se esaminasse il documento con il Blocco Note, però, potrebbe vedere il file trafugato. Poi, quando Bob salva il documento, il file diventa parte del documento salvato. Lui lo spedisce indietro ad Alice, e Alice è riuscita a rubare il file.

secondo è molto più simile ad una guerra di religione. Rimango continuamente esterrefatto di fronte a quante persone (che stiano da una parte o dall'altra sulla questione armi e piloti) argomentino in base alle proprie conclusioni invece di valutare razionalmente i fatti. I commenti che seguono sono quelli che io ritengo contribuiscano all'analisi, e che sono privi di "teologie". Ed è assai improbabile che pubblicherò commenti a questi commenti il prossimo mese. È un genere di discussione che tollero fino a un certo punto.

Da: Blake Leverett <bleverett@att.net>
Oggetto: Armare i piloti di linea

La sua prima e seconda obiezione riguardano la gestione delle pistole che i piloti dovrebbero portare con sé: come fanno a circolare le pistole, e come possiamo essere certi che non vengano lasciate in giro?

C'è soltanto una risposta a queste domande: un pilota porterà con sé la propria pistola, la porterà addosso. Non devono esserci ripostigli o altri tipi di deposito, perché, come lei ha detto, bisogna evitare che le armi vengano abbandonate sull'aereo. Nessuna persona competente perderebbe di vista la propria arma. Il pilota conserva sempre la pistola in una fondina su misura, anche quando lascia la cabina di pilotaggio. Molti piloti di linee commerciali hanno un addestramento militare e sono già pronti all'uso di rivoltelle. Fra parentesi, per un malintenzionato è più facile impossessarsi della pistola di un poliziotto, perché è in una fondina aperta e visibile. Nel caso di un pilota bisogna prima individuarla (potrebbe essere in una fondina ascellare, o dietro la schiena, o alla caviglia, destra o sinistra) e si deve entrare in contatto fisico col pilota per rubarla.

Niente di tutto ciò è teoria. Migliaia di persone oggi portano addosso armi nascoste, sia ufficiali di polizia che privati cittadini. E vi sono anche centinaia di pistole dietro i posti di blocco negli aeroporti. Prima dell'11 settembre, almeno, c'erano molte persone che potevano portare armi anche all'interno della zona "sicura". Bastava che mostrassero un distintivo e potevano superare tranquillamente le guardie di "sicurezza".

Ciò che ha detto sull'addestramento dei piloti è discutibile. Molti piloti sono già addestrati dall'esercito. Questo è un programma volontario. Sarebbe stupido costringere un pilota a portarsi addosso un'arma contro la sua volontà. Vi sono diversi programmi di addestramento a seconda del tipo di uso che si deve fare di una rivoltella, e immagino che i piloti dovrebbero passare un esame quantomeno rigoroso.

Infine, le pistole sono molto più utili come deterrente che non come strumenti per contrastare i dirottatori. Una volta che un gruppo di dirottatori si trova sull'aereo con l'intento di prenderne possesso, accadranno cose spiacevoli a prescindere dalle soluzioni intraprese. Credo che qui la parte emotiva stia sorpassando quella logica: la gente vuole permettere la presenza di ufficiali di volo armati, ma non vuole che i piloti siano armati. I piloti hanno già le nostre vite nelle loro mani, e sono professionisti addestrati ad agire con rapidità nelle situazioni critiche. Sono molto più qualificati ad essere armati di un ufficiale Rambo qualsiasi.

Da: Ron Lautmann <ron_lautmann@pacbell.net>
Oggetto: Armare i piloti di linea

Centinaia, forse migliaia di pistole vengono trasportate al sicuro sulle linee aeree statunitensi al giorno d'oggi. Ogni funzionario di polizia che ha prestato giuramento, che si reca da un posto all'altro in aereo, viaggia armato. Gli agenti di FBI, Servizi Segreti, Advanced Tactical Fighters, e molti altri, viaggiano armati e riescono sempre a far passare le loro rivoltelle attraverso gli aeroporti e ad averle con sé in aereo. Quando arrivano al controllo non fanno altro che mostrare le loro credenziali e passare indisturbati. La soluzione più ovvia al problema di

armare i piloti sarebbe quella di lasciare che anch'essi viaggino armati, proprio come i funzionari di polizia. Magari un giorno lo diventeranno pure.

Molti piloti hanno espresso vivo interesse nel portare pistole in cabina di pilotaggio. Questo fatto è attestato da organizzazioni come l'APSA (cfr. <<http://www.secure-skies.com>>). Da questo uno dovrebbe dedurre che i piloti riceverebbero un adeguato addestramento sull'uso sicuro di una pistola, specialmente in caso di un attacco. Quei piloti che non intendessero seguire tale addestramento potrebbero uscire volontariamente dal programma e non portare armi con sé.

Gli eventuali dirottatori non avrebbero modo di sapere quali piloti sono armati, per cui non avrebbero alcun vantaggio dal sapere che alcuni piloti non lo sono.

Le notizie ci informano costantemente del fatto che, anche con controlli più severi negli aeroporti, esiste una possibilità su quattro che un'arma oltrepassi il sistema di controllo senza essere rilevata. Credo che armare i piloti possa contribuire a proteggerci da questa triste casistica.

Fra l'altro, a quanti poliziotti viene rubata la pistola, come lei fa notare? Non credo vi saranno molti dirottatori che si affideranno a questo sistema per ottenere un'arma. Per un dirottatore, tendere un agguato ad un pilota mentre si dirige dalla cabina di pilotaggio alla toilette, è una situazione troppo incerta.

Infine, se l'ultima linea di difesa per proteggere il paese contro un aereo di linea dirottato è quella di essere abbattuti da un caccia F16, preferirei che il pilota del mio aereo sia armato, invece di rischiare di essere abbattuto.

Da: "Bill Nickless" <bill@nonick.org>
Oggetto: Armare i piloti di linea

Migliaia di rivoltelle già si trovano sugli aerei e negli aeroporti. Mi capita di vederle in continuazione addosso a membri del personale di sicurezza ai posti di controllo, e si sa che gli ufficiali di volo viaggiano armati. Molti dipendenti di agenzie federali, compresi quelli della Smithsonian Institution, le possono portare e infatti portano con sé le proprie armi quando viaggiano. Ufficiali della polizia di stato, in occasione di viaggi di lavoro (in qualità di guardie del corpo di ufficiali di stato, per esempio), portano armi con sé. Ufficiali di altre nazioni sono abitualmente armati per proteggere i diplomatici e funzionari governativi che viaggiano in aereo.

I piloti di linea sono già fra le persone più addestrate ed attentamente scelte che vi siano in circolazione. Devono avere a che fare quotidianamente con macchinari complessi. Il loro compito principale è quello di proteggere le vite e l'incolumità dei loro passeggeri, non soltanto quello di guidare aerei. Attualmente la loro unica arma di difesa è l'ascia "in caso di incendio" nella cabina di pilotaggio.

Questa dei piloti di linea armati non è un'idea nuova. Infatti, per anni la legge federale ha imposto loro di portare un arma con sé, dato che le linee aeree commerciali trasportavano la posta statunitense. Questo episodio riportato dallo Houston Chronicle (<<http://www.chron.com/cs/CDA/story.htm?metropolitan/1087467>>) è solo un esempio di una situazione dove un dirottatore armato è stato fermato con successo da un pilota di linea armato.

Da: "ADP" <adp@commspeed.net>
Oggetto: Armare i piloti di linea

In qualità di comandante di volo in pensione, con più di 34 anni di servizio, sono completamente d'accordo con lei in merito alla questione di armare i piloti di linea. Penso che sia l'idea più sciocca sin dai tempi del PC Jr.

Siamo una nazione di persone di scarsa attenzione e di ancor più scarsa memoria. Il mestiere di un pilota è quello di pilotare il proprio velivolo. Punto.

Prima dell'11 settembre, a noi piloti si insegnava di accettare le richieste dei dirottatori. Questo sistema ha funzionato per tanti anni. Con l'arrivo di terroristi suicidi, il sistema deve essere abbandonato. Il comandante di un volo di linea è responsabile del suo equipaggio, ovviamente, ma soprattutto è responsabile della sicurezza del suo aereo e dei passeggeri. Mi dispiace che, in alcune circostanze, un comandante possa mettere a repentaglio la vita di un membro dell'equipaggio. Ma mi stupisco del fatto che i piloti di linea non si concentrino sul controllo del loro aereo. Un conflitto a fuoco a trentamila piedi di altezza in cui venga coinvolto un pilota significa che soltanto una sola persona, l'altro pilota, stia guidando l'aereo. (Non vi sono quasi più equipaggi con tre piloti, ormai).

Si rendano gli sportelli della cabina inespugnabili. Si offra un'uscita di emergenza sicura per i piloti in caso di sciagura. Si lasci fare ai piloti il proprio mestiere mentre altri si occupano della sicurezza.

Da: Norman Yarvin <norman.yarvin@snet.net>
Oggetto: Armare i piloti di linea

Nell'ultimo numero di Crypto-Gram lei ha elencato una serie di problemi connessi all'armare i piloti. Ritengo che siano delle ottime obiezioni ad un programma che contempra l'obbligo di portare pistole. Ma se il programma prevedesse semplicemente la scelta da parte dei piloti di essere armati o meno, molti di quei problemi si attenuerebbero. I piloti che decidessero di portare armi con sé sarebbero coloro che in precedenza si erano curati di tattiche militari, e che erano buoni tiratori (si tenga presente che una buona percentuale di piloti sono stati militari). Per ridurre la possibilità di venire disarmati, si potrebbe dar loro l'opportunità di portare addosso pistole nascoste, o di lasciare la propria arma in cabina mentre sono alla toilette. Un terrorista non potrebbe sapere con certezza se i piloti sono armati o addirittura se vi sono armi a bordo.

Per ciò che riguarda il protocollo del portare armi a bordo, in un sistema dove le armi ai piloti fossero facoltative, ogni pilota sarebbe responsabile della propria arma in ogni momento. In questo modo, egli potrebbe scegliere una pistola e una fondina di suo gradimento, e che possa nascondere al meglio. Tutto questo non sarebbe molto diverso dal modo in cui gli ufficiali di volo portano armi a bordo.

Penso che un progetto del genere avrebbe più possibilità di essere utile che di portare danno, anche se non sarebbe una panacea. Ma devo ammettere che sarà difficile che venga implementato: in questo paese la mentalità del controllo è troppo forte, al punto che se si farà qualcosa, sarà probabilmente un caso del tipo "oggi, proibito; domani, obbligatorio".

Da: Allen Gordon <a.gordon@cablelabs.com>
Oggetto: Armare i piloti di linea

Ho chiesto ad un amico, che è stato pilota delle United Airlines per più di 35 anni. Riguardo a questo problema lui ha risposto: "Hmm, vediamo, io sono destrimano. Sono seduto nel sedile di sinistra. Estraggo la pistola con la mano destra, ma siccome sono legato al sedile non posso girarmi più di tanto, per cui potrei finire con lo sparare al co-pilota!"

Da: Ric Woodson <cmesoft@data-experts.com>
Oggetto: Armare i piloti di linea

In risposta al dibattito riguardante le armi in cabina di pilotaggio, vorrei suggerire un'alternativa alla quale nessuno finora ha dato migliore soluzione. Per tutta la lunghezza dei lati dell'aereo dove sono i passeggeri, si monti un condotto dentro un altro condotto. Ogni condotto presenta delle aperture, per tutta la sua lunghezza, di circa 1/3 del suo diametro. Il condotto esterno è statico, quello interno può ruotare su una posizione di aperto solo su comando della cabina.

Nel tubo interno sono disposte delle mazze da baseball grandi la metà di quelle regolamentari, adagiate con gli estremi a contatto. Una volta che i condotti sono aperti, il passeggero accanto al finestrino ha accesso alle mazze. Queste possono essere utilizzate per attaccare o per difendersi. Ogni fila di sedili avrebbe quindi due mazze per fila. Più che sufficienti per riconquistare il controllo del velivolo. Vi sarebbero troppe mazze da requisire e da gestire da parte dei "terroristi" (si è mai provato a raccogliere più di quattro mazze per volta?). Non c'è possibilità che queste armi facciano cilecca. Nulla che possa distrarre i piloti dal loro lavoro. Troppo piccole da usarsi per attaccare gli sportelli di sicurezza. Per le autorità è molto semplice inventariarle e ritirarle dopo l'atterraggio.

Un sistema poco costoso e relativamente semplice da installare. Dopotutto chi ha più esperienza con una buona mazza da battitore se non un passeggero americano? Perché non dare ai passeggeri l'opportunità di ribellarsi, se è necessario? Si lascino a casa gli ufficiali e si risparmi il denaro. Si lascino da parte le soluzioni ad alta tecnologia, perché questo non è un problema di alta tecnologia. So che può sembrare un po' troppo radicale, ma riflettiamoci su.

Da: Jay Ackroyd <jayac@dbsinyc.com>
Oggetto: Armare i piloti di linea

Tutto molto giusto e ben detto, ma credo che lei abbia trascurato un particolare, in riferimento sia ai piloti che agli ufficiali. Una volta che c'è una pistola a bordo, l'impresa sta nel sottrarla alla persona che la possiede ed usarla per dirottare l'aereo. Bisogna ricordare che i terroristi agiscono in squadre di quattro o cinque persone, a cui non importa nulla di morire. La prima parte dell'impresa è identificare chi è armato e dove tiene l'arma, il che richiede il sacrificio di uno dei membri della squadra. Questo fatto può essere sfruttato come parte di un piano precedentemente elaborato per impossessarsi dell'arma.

Come lei ha detto in quell'articolo molto interessante sull'Atlantic, la cooperazione fra i membri dell'equipaggio e i passeggeri per prevenire un dirottamento è la nostra contromisura più efficace per evitare che gli aerei vengano usati come missili. Armi a bordo degli aerei non potenziano questa contromisura, semmai possono indebolirla.

Da: Michael Ortega-Binderberger <miki@ics.uci.edu>
Oggetto: Armare i piloti di linea

Un fattore che lei non ha menzionato, e che può complicare le cose, riguarda gli altri paesi. Sono uno studente internazionale e mi trovo negli Stati Uniti. Provengo dal Messico, e posso dirle che laggiù le pistole sono assolutamente proibite. Allo stesso modo, molti paesi potrebbero vietare ai piloti americani l'uso delle armi quando si trovassero nel loro territorio (e anche vietandole, la situazione sarebbe comunque problematica). Analogamente, molte compagnie aeree estere potrebbero non armare i propri piloti, anche per i voli verso gli USA. Conseguenza: se fosse semplice controllare quali aerei su quali rotte sono "armati" e quali no, questo stesso fatto offrirebbe una porta spalancata per chi intendesse abusarne.

Da: "Nicholas C. Weaver" <nweaver@CS.Berkeley.EDU>
Oggetto: Armare i piloti di linea

Vi sono ora molte nuove opportunità per scongiurare un dirottamento (specialmente quei passeggeri intenzionati a mutilare qualsiasi potenziale terrorista, fra le altre cose). Ma non vi sono più opportunità che possano evitare che un pilota ribelle faccia schiantare l'aereo, come pare essere accaduto nel caso della Egypt Air.

Una pistola in cabina faciliterebbe questo tipo di attacco, perché il pilota ribelle (armato) ucciderebbe le sue controparti e farebbe schiantare l'aereo, invece di dover combattere contro il resto dell'equipaggio della cabina.

Da: Niels Ferguson <niels@ferguson.net>
Oggetto: Palladium

Microsoft dichiara molti vantaggi per Pd, alcuni di questi sono connessi al permettere il Digital Rights Management (DRM). Tuttavia, molti di quei benefici possono essere ottenuti attraverso l'hardware già esistente. Tutte le CPU Intel sin dalla 286 hanno sempre avuto un'ottima separazione hardware dei task. È solo una scelta di Microsoft quella di non avvalersi di tale funzionalità che ha portato ad avere un unico blocco di codice interdipendente.

Le CPU Intel possono proteggere un programma dall'altro. Si possono realizzare driver sicuri che non mandano più in crash il computer. Ma il sistema operativo di base avrà sempre il pieno controllo della macchina. Per cui si potrà proteggere un programma dall'altro, e si potrà proteggere l'utente dal software maligno, ma l'utente avrà sempre il completo controllo del computer.

La novità di Pd è quella di sottrarre questo controllo all'utente. Esso "permette" all'utente di lasciare parte del suo controllo alla macchina, e di darla ad un programma. Questo naturalmente fa parte dei requisiti per il DRM, ma non riesco proprio ad immaginare a quale altra applicazione. Hanno parlato di cose come il software per applicazioni bancarie, ma è una sciocchezza. Abbiamo dell'ottima crittografia per gestire quel tipo di minaccia, ed usare Pd per applicazioni bancarie sarebbe molto pericoloso. Dopotutto il processore di Pd non è protetto contro gli attacchi fisici, per cui occorrerebbe affidarsi comunque al proprietario del computer.

Sono circolate informazioni sbagliate sul fatto che non sia possibile cambiare l'intero sistema operativo Windows e che quindi Pd sia necessario per creare una sorta di micro-kernel sotto il sistema operativo. Questo non è vero. Si può fare la stessa cosa su hardware Intel: VMware è un buon esempio. Microsoft può raggiungere le stesse caratteristiche di sicurezza (tranne il DRM) utilizzando l'hardware già esistente e il medesimo sforzo nello sviluppo del software.

La mia conclusione: la sola ragione che giustifica Pd è il DRM. Tutto il resto è soltanto fumo negli occhi, o sciocchezze. È sempre difficile capirne la differenza.

Da: "Nicholas C. Weaver" <nweaver@CS.Berkeley.EDU>
Oggetto: Palladium

Le parti dedicate alla protezione del proprietario/utente del computer non richiedono hardware: si affidano al fatto che il sistema operativo faccia il suo dovere, tenendo d'occhio un eventuale codice "alieno". Non esiste nulla che eviti che sugli attuali sistemi vengano imposti una firma di codice universale per l'autenticazione della fonte, o un forte sandboxing, ecc. L'hardware è necessario per prevenire gli attacchi che si basano sul debugging.

CVD: l'hardware viene progettato in primo luogo per NON avvantaggiare il proprietario/utente, ma per limitarne la capacità di manipolare il sistema. Questa, per molti, è forse una buona cosa?

Da: Fredrik Viklund <fredrikv@biotech.kth.se>
Oggetto: Riconoscimento facciale

Gli insuccessi del riconoscimento facciale come mezzo per identificare terroristi mi ha fatto pensare a certi parallelismi nell'ambito delle diagnosi mediche, dove i problemi sono simili.

Le richieste di un metodo diagnostico sono molto differenti e dipendono da questi punti:

- Devono essere evitati i falsi positivi o i falsi negativi?
- La malattia è diffusa oppure rara?
- Lo strumento diagnostico si rivela costoso per il paziente in termini monetari o di dolore?

Per una malattia diffusa (come il parassita ascaris, non letale), dove il trattamento è economico e relativamente indolore per il paziente, uno strumento di diagnosi semplice e poco costoso è adeguato. Basso costo e nessun dolore per il test e per il trattamento significa non avere problemi se appaiono alcuni falsi negativi o positivi. Diciamo che il 50% della popolazione è infetta. Quindi, un tasso del 2% di falsi positivi non avrà molto effetto sui costi del trattamento. Un tasso del 2% di falsi negativi, tuttavia, farà sì che molte persone (l'1% della popolazione) siano ancora in giro a diffondere la malattia.

Una malattia rara e mortale, con un tipo di trattamento doloroso, d'altra parte, richiede uno strumento diagnostico con una scarsissima presenza di falsi positivi e negativi. Se solo lo 0,1% della popolazione contrae la malattia, un tasso del 2% di falsi positivi aumenterà di venti volte il costo e il dolore per il trattamento. Un tasso del 2% di falsi negativi priverà del trattamento "soltanto" lo 0,002% della popolazione, e il 98% degli infetti verrà rilevato. Questo è il caso parallelo al terrorismo.

Questo ha un tremendo impatto su quali metodi siano adeguati per diagnosticare malattie (e terroristi), ed io spero vivamente che le persone responsabili di diagnosticare il terrorismo abbiano studiato bene epidemiologia prima di iniziare il trattamento.

Da: Martin Spamer <martin_spamer@kingston-comms.co.uk>
Oggetto: Licenza di hacking

Per quanto riguarda i suoi commenti in "Licenza di hacking", vorrei far presente che i "contrattacchi", così come sono stati proposti da RIAA ed MPAA sarebbero illegali in parecchi altri paesi.

Infatti un tale comportamento sarebbe illegale nel Regno Unito, come sancito dalla Sezione 1 del Computer Misuse Act del 1990:

(1) Un individuo è passibile di reato se: (a) permette ad un computer di eseguire una qualsiasi funzione con l'intento di ottenere l'accesso a qualsiasi programma o dati conservati in altro computer; (b) l'accesso che intende ottenere non è autorizzato; e (c) egli è conscio, nel momento in cui permette al computer di eseguire tale funzione, di ciò che sta facendo.

(2) L'intento che un individuo deve avere per commettere reato, secondo questa sezione, non deve necessariamente essere diretto verso: (a) un programma o una serie di dati particolari; (b) un programma o una serie di dati di un particolare genere; o (c) un programma o una serie di dati conservati in un computer particolare.

(3) Un individuo passibile di reato secondo i termini di questa sezione sarà soggetto, su giudizio sommario, a prigionia per un periodo non superiore a sei mesi o ad una ammenda non superiore al livello 5 della misura standard, o ad entrambi.

<http://www.hmsso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm>

Dato che questa legislazione del Regno Unito è il risultato di impegni contrattuali a livello europeo (<<http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=185>>), una simile legislazione esiste (o esisterà) in tutta Europa.

Se le proposte statunitensi verranno accettate, come pare possibile, possiamo aspettarci una situazione opposta al caso Dmitri Sklyarov, con i funzionari di RIAA ed MPAA che vengono arrestati, incarcerati o estradati da qualche parte in Europa.

Da: "David Banes" <dbanes@symantec.com>

Oggetto: Licenza di hacking

Una parte del progetto di legge dice: "il detentore di copyright non sarà ritenuto responsabile in nessuna causa penale o civile per aver disabilitato, interferito con, bloccato, dirottato, o danneggiato in altro modo la distribuzione, la proiezione, la rappresentazione o la riproduzione non autorizzata del proprio lavoro sotto copyright su un network peer-to-peer di scambio dati pubblicamente accessibile, se questo danno non altera, cancella, o deteriora in altro modo, e senza autorizzazione, l'integrità di un qualsiasi file o dato contenuto nel computer di chi scambia i file."

La parte conclusiva è la chiave per comprendere il progetto di legge, visto che i detentori di copyright si daranno la zappa sui piedi se rilasceranno virus che "alterano, cancellano, o deteriorano in altro modo, e senza autorizzazione, l'integrità di un qualsiasi file o dato contenuto nel computer di chi scambia i file" perché i file verranno alterati (i log, ecc.) e gli eseguibili saranno mutati se un virus è attivo.

Ciò che mi pare di capire dal progetto di legge è che permetta il blocco o la disattivazione dei network peer-to-peer a livello network, non a livello del singolo utente che scambia i file.

Da: Marty Levy <marty@transmeta.com>

Oggetto: Carnival Booth

Mi è piaciuto moltissimo l'ultimo Crypto-Gram, soprattutto la descrizione di M\$ Pd. Vorrei però mettere in discussione "Carnival Booth", che lei ha descritto come "un buon lavoro". Il lavoro in realtà era abbastanza interessante, ma sembrava essere basato su almeno un assunto completamente errato, e che infine pare annullare le conclusioni più importanti dello studio. Questa falsa assunzione è talmente sfacciata che devo sospettare che gli autori abbiano un ordine del giorno politico/sociale, e mi rincresce che lei sembri sostenere il loro lavoro, visto che non regge nemmeno al più modesto esame critico.

Gli autori dello studio partono dall'assunzione che interrogando il CAPS e quindi determinando il profilo di quei malintenzionati che è improbabile siano presi di mira, l'organizzazione terroristica possa quindi preferire individui di basso profilo. Posso essere d'accordo che in un mondo in cui i terroristi avessero una popolazione davvero casuale o enormemente vasta e diversificata da cui attingere tali individui, questa tecnica sarebbe proficua. Gli autori cercano di sostenere l'assunzione secondo cui questa strategia è efficace nella sezione 3.3, facendo il nome di cinque recenti "terroristi" - Lindh, Reid, Helder, Kaczynski e McVeigh. La loro asserzione, basata sull'osservazione che questi cinque terroristi esistono, è che "ai terroristi non mancano di certo delle differenze".

Prima di tutto questi cinque hanno almeno una caratteristica in comune (e forse anche altre): sono tutti maschi. Non ho alla mano i dati in merito all'età, ma credo che la maggior parte di essi fosse sotto i 40 anni quando commise i primi atti terroristici.

Ma, cosa ancora più importante, la popolazione da cui le più importanti organizzazioni terroristiche possono attingere, fra tutte le persone a cui non importa finire arrestate o morte, probabilmente non è così diversificata. Di certo, coloro i quali hanno perpetrato i fatti dell'11 settembre avevano tutti caratteristiche comuni, che sono anche relativamente poco frequenti nella popolazione generale.

Una volta che i terroristi prevedessero che le vecchie signore di origini statunitensi con nomi non arabi hanno minori probabilità di essere individuate dal CAPS rispetto a giovani uomini nati in Medio Oriente con nomi arabi, come metterebbero in pratica queste informazioni?

Lo studio è arrivato vicino alle giuste conclusioni: qualsiasi esperto terrorista è ora in grado di sapere che certi tratti somatici avranno maggiori probabilità di attirare attenzione, e i terroristi cercheranno quindi di usare e reclutare persone prive di quei tratti (oppure faranno in modo di nascondere quei tratti). Per questo motivo, le ispezioni casuali dovrebbero aver luogo, ma senza sostituire completamente quelle mirate.

Sono sorpreso che lei non abbia rilevato una grave mancanza dello studio a livello logico: se i terroristi riescono a rilevare che TUTTE le ispezioni sono casuali, allora potranno tornare ad affidarsi alla vasta popolazione di cui dispongono (e che ha particolari caratteristiche). Questa è una problematica prototipica nel controspionaggio, e lei avrebbe dovuto evidenziarla.

Questo studio sarebbe stato molto più utile se gli autori avessero cercato di delineare come ottimizzare un misto di ispezioni casuali e mirate. Spero che la FAA abbia messo in conto l'aiuto di buoni statistici per farlo già da ora.

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

CRYPTO-GRAM è una newsletter mensile gratuita che offre riassunti, analisi, approfondimenti, e commenti sulla sicurezza informatica 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 la rivista interessante. Viene concessa l'autorizzazione a ristampare CRYPTO-GRAM, a condizione che sia stampata integralmente.

CRYPTO-GRAM è realizzata da Bruce Schneier. Schneier è il fondatore e CTO di Counterpane Internet Security, Inc., autore di "Secrets and Lies" e di "Applied Cryptography" e inventore degli algoritmi Blowfish, Twofish e Yarrow. È membro del comitato consultivo dell'Electronic Privacy Information Center (EPIC). Scrive spesso e tiene conferenze in merito alla sicurezza informatica e alla crittografia.

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.

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

Copyright (c) 2002 by Counterpane Internet Security, Inc