

CRYPTO-GRAM
15 agosto 2002

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:

[Palladium e il TCPA](#)

[Le ristampe di Crypto-Gram](#)

[Il Canile: Cedium](#)

[Counterpane -- un'importante ricerca](#)

[Licenza di hacking](#)

[News](#)

[Le news di Counterpane](#)

[Armare i piloti delle linee aeree](#)

[Commenti dei lettori](#)

** **

Palladium e la TCPA

Era da parecchio tempo che non si scriveva così tanto in merito alla sicurezza informatica come da quando è apparsa l'iniziativa di Microsoft per la sicurezza, chiamata Progetto Palladium. L'elenco di link riguardanti commenti, analisi e opinioni che fornisco in calce all'articolo è piuttosto lungo. Il che è quantomeno interessante, dato che non si conosce molto dei dettagli su che cosa sia o come funzioni. Molto di questo viene ricavato leggendo fra le righe dei vari comunicati stampa, o da conversazioni che ho avuto con persone di Microsoft (nessuno di loro sotto accordo di non divulgazione), o da conversazioni con persone che a loro volta hanno avuto conversazioni con altre. Ma siccome non possiedo dati certi, tutto ciò che segue potrebbe essere errato.

Palladium (come i chimici, Microsoft lo abbrevia in "Pd") è, in un qualche modo, l'implementazione di Microsoft delle specifiche TCPA. Il "qualche modo" dipende da come rispondono coloro a cui ci si rivolge; alcuni dicono che ha attinenza, altri dicono che vengono svolte cose simili ma che non hanno attinenza, altri ancora dicono che Pd è, a tutti gli effetti, il tentativo di Microsoft di rimpiazzare le specifiche della TCPA. La TCPA è la Trusted Computing Platform Alliance, un'organizzazione con poco meno di 200 associati (un elenco davvero impressionante) che cerca di realizzare un sistema informatico sicuro. Le specifiche TCPA 1.1 sono state pubblicate, ed è possibile ottenere la versione 1.2, a patto di non divulgarla. Pd non segue esattamente queste specifiche, ma ne segue le linee, in un certo senso.

Pd è stato sotto sviluppo per molto tempo, a partire almeno dal 1997. La migliore descrizione tecnica è il riassunto di un incontro con gli ingegneri Microsoft da parte di Seth Schoen di EFF (vedi link in fondo). Non è mia intenzione entrare nei dettagli, anche perché i sistemi equipaggiati con una prima versione di Pd non verranno distribuiti prima del 2004, ed è probabile che nel frattempo i dettagli possano cambiare.

Essenzialmente, Pd è il tentativo da parte di Microsoft di costruire un sistema informatico "trusted" (ho parlato di questo concetto in "Secrets and Lies", pp. 127-130; vi si faccia riferimento per meglio seguire il discorso). L'idea è che i diversi utenti del sistema abbiano delle limitazioni sulle possibilità d'azione, e che siano vicendevolmente isolati. Questo è impossibile da ottenere solamente via software, e Pd infatti è una combinazione hardware/software. Pd influisce sulla

CPU, sul chip set della scheda madre, sui dispositivi di input (mouse, tastiera, ecc.), e sui dispositivi di output (processore grafico, ecc.). In più è richiesto un nuovo chip: un processore sicuro contro i tentativi di manomissione.

Microsoft ha prontamente riconosciuto che Pd non potrà essere sicuro contro attacchi hardware. Stanno facendo alcuni sforzi per rendere più difficoltoso estorcere informazioni dal processore sicuro, ma non vi stanno spendendo moltissime energie. Presumono che le difese contro la manomissione verranno sconfitte. Ed è loro intenzione progettare il sistema in modo che gli attacchi hardware non finiscano col provocare forzature su vasta scala, che il sabotare una macchina non aiuti in alcun modo a sabotarne altre.

Pd offre protezione contro due principali classi di attacco. Gli attacchi software automatizzati (i virus, i Trojan, gli exploit effettuati via rete) vengono controllati poiché una vulnerabilità forzata in una parte del sistema non possa influire sul resto del sistema. E gli attacchi software a livello locale (ad es. utilizzando dei debugger per indagare su cosa c'è di aperto) vengono isolati grazie alla separazione delle parti del sistema.

Vi sono delle funzionalità di sicurezza che legano i programmi e i dati alla CPU e all'utente, e che li criptano per ragioni di privacy. Ciò probabilmente è necessario al funzionamento di Pd, ma viene ad avere un effetto collaterale che, ne sono certo, rende Microsoft alquanto eccitata. Come per libri, mobili e capi di vestiario, chi compra nuovo software può rivenderlo quando non gli occorre più. Le persone hanno il diritto di farlo -- negli Stati Uniti viene chiamato "First Sale Doctrine" -- tuttavia l'industria del software ha da sempre affermato che i programmi non vengono venduti, ma licenziati, e non possono essere ceduti. Quando qualcuno venderà un sistema munito di Pd, è probabile che resetterà le proprie chiavi, in modo che la sua identità non possa essere utilizzata e i file non possano essere letti. Questo servirà inoltre ad azzerare tutto il software che ha acquistato. Il risultato finale potrebbe essere che gli utenti non siano più nelle condizioni di rivendere il software, anche volendo.

Pd è vincolato inesorabilmente con la gestione dei diritti digitali (Digital Rights Management, DRM). Il vostro computer presenterà diverse partizioni, ognuna delle quali sarà in grado di leggere e scrivere i propri dati. Non c'è nulla in Pd che impedisca a qualcun altro (Disney, Microsoft, il vostro capo) di impostare una partizione sulla vostra macchina e di inserirvi dati a cui non potete avere accesso. Microsoft ha ripetutamente dichiarato che non ha intenzione di affidare il mandato al DRM, né di cercare di controllare i sistemi DRM, ma Pd è stato chiaramente progettato tenendo presente il DRM.

Pare che vi siano buoni controlli per quanto concerne la privacy, di gran lunga migliori di quanto mi sarei aspettato. Microsoft ha dichiarato che renderà pubblico il codice centrale, in modo che possa venire riesaminato e verificato. Finalmente Microsoft si è resa conto che vi sono molte persone intenzionate a svolgere il loro lavoro sulla sicurezza gratuitamente.

Non è facile individuare le implicazioni di Pd a livello di antitrust. Molte persone ne hanno scritto. Microsoft realizzerà Pd in modo che non sia possibile farvi girare Linux? No, non oserà farlo. Prenderà protocolli Internet standard per sostituirli con protocolli proprietari Microsoft? Non credo. Occorrerà un dispositivo predisposto per Pd (il sistema è progettato per funzionare sia su computer general-purpose che su dispositivi multimediali specializzati) per visionare materiale protetto da copyright? Molto probabilmente. Farà in modo di imporre i propri brevetti di Pd il più possibile? Quasi certamente.

Molte informazioni riguardanti Pd verranno rilasciate da Redmond nei prossimi anni, alcune vere, altre no. Molte cose cambieranno, per poi cambiare nuovamente. Il sistema finale potrebbe non assomigliare per nulla a ciò che abbiamo visto finora. Tutto questo è normale e bisogna aspettarselo, ma mentre continuerete a leggere di questo progetto, assicuratevi di tenere sempre presenti alcune cose.

1. Un computer "trusted" non significa un computer fidato. La definizione di sistema trusted del Dipartimento della Difesa americano è di un sistema che può infrangere la vostra politica di sicurezza; per esempio, un sistema a cui si è obbligati ad affidarsi perché non si hanno alternative. Pd avrà delle caratteristiche di un sistema sicuro; si deve ancora stabilire se queste siano sicure e attendibili o meno.

2. Quando si pensa ad un computer sicuro, la prima domanda che dovete porvi è: "sicuro per chi?" Microsoft ha affermato che Pd permette al proprietario del sistema di impedire che altri utenti inseriscano le proprie aree sicure all'interno del computer. Ma in realtà, quali sono le probabilità che accada una cosa del genere? La NSA sarà certamente in grado di acquistare computer con Pd implementato e renderli sicuri da ogni influenza esterna. Dubito però che si riesca ad ottenere lo stesso risultato da parte vostra o mia, continuando a beneficiare della ricchezza di Internet. A Microsoft non importa granché della vostra opinione; ad essa importa ciò che pensano RIAA ed MPAA (le organizzazioni statunitensi dei produttori discografici e cinematografici, ndr). Microsoft non può permettersi che

l'industria dei media non possa rendere disponibili i propri prodotti su piattaforma Microsoft, e farà tutto ciò che potrà per venirle incontro. Spesso vi è un divario considerevole fra ciò che si può ottenere in teoria (che è quello su cui insiste Microsoft nelle discussioni su Pd) e ciò che si potrà avere in pratica. Qui è dove risiede il pericolo principale.

3. Come ogni altra cosa prodotta da Microsoft, Pd avrà delle falle di sicurezza talmente grandi da farci passare un camion, e saranno parecchie. Quelle a livello hardware saranno più difficili da sistemare. Assicuratevi di separare tutto ciò che è promessa su Pd da parte delle pubbliche relazioni di Microsoft, da ciò che sarà in effetti Pd 1.0.

4. Fate attenzione al punto di vista dell'antitrust. Vi posso garantire che Microsoft crede che Pd sarà un modo di aumentare la sua quota di mercato, non di incrementare la concorrenza.

Vi sono parecchie ottime cose in Pd, e vi è molto in Pd di mio gradimento. Ma vi è anche molto che non approvo e che mi spaventa. La mia paura è che Pd ci porterà ad un punto in cui i nostri computer non saranno più nostri, ma saranno posseduti da una serie di aziende e compagnie tutte interessate a una parte del nostro portafoglio. Se Pd ha la possibilità di spianare la strada a un tale scenario, questo è un male per la società. Non mi importa che vi siano aziende che mi vendano, affittino o licenzino programmi, ma la perdita della potenza, possibilità e flessibilità del computer è un prezzo troppo alto da pagare.

<<http://www.theregus.com/content/4/25378.html>>
<<http://www.msnbc.com/news/770511.asp?cp1=1>>
<http://news.com.com/2100-1001-938973.html?tag=cd_mh>
<<http://www.eweek.com/article2/0,3959,267488,00.asp>>
<<http://www.internetweek.com/story/INW20020626S0007>>
<<http://www.osopinion.com/perl/story/18379.html>>
<<http://www.infoworld.com/articles/hn/xml/02/06/25/020625hnpalladium.xml>>
<<http://www.newscientist.com/news/news.jsp?id=ns99992449>>
<<http://www.washingtonpost.com/wp-dyn/articles/A51780-2002Jun26.html>>
<<http://www.theregus.com/content/4/25630.html>>
<<http://www.internetweek.com/story/INW20020626S0007>>

Il riassunto di Seth Schoen sull'incontro:

<<http://vitanuova.loyalty.org/2002-07-03.html>>

Opinioni:

<<http://www.nytimes.com/2002/07/04/business/04SCEN.html>>
<<http://online.securityfocus.com/columnists/96>>
<<http://zdnet.com.com/2102-1107-942699.html>>
<<http://online.securityfocus.com/columnists/93>>
<<http://zdnet.com.com/2102-1107-939817.html>>
<<http://www.theregister.co.uk/content/4/25843.html>>
<<http://www.pbs.org/cringely/pulpit/pulpit20020627.html>>

Ross Anderson sulla TCPA e Palladium:

<<http://www.cl.cam.ac.uk/users/rja14/tcpa-faq.html>>
<<http://www.theregus.com/content/4/25415.html>>

Il sito Web della TCPA:

<<http://www.trustedcomputing.org/tcpasp4/index.asp>>

** **

Le ristampe di Crypto-Gram

Crypto-Gram è attualmente al suo quinto 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.counterpane.com/crypto-gram.html>>. Quella che segue è una selezione di articoli apparsi in questo mese gli anni scorsi.

Code Red:

<<http://www.counterpane.com/crypto-gram-0108.html#1>>

La protezione del copyright nel Mondo Digitale:

<<http://www.counterpane.com/crypto-gram-0108.html#7>>

Vulnerabilità, divulgazione e fix basate su virus:

<<http://www.counterpane.com/crypto-gram-0008.html#2>>

Bluetooth:

<<http://www.counterpane.com/crypto-gram-0008.html#8>>

Un "cracker" hardware DES:

<<http://www.counterpane.com/crypto-gram-9808.html#descracker>>

Sistemi biometrici: verità e fantasie:

<<http://www.counterpane.com/crypto-gram-9808.html#biometrics>>

Back Orifice 2000:

<<http://www.counterpane.com/crypto-gram-9908.html#BackOrifice2000>>

Servizi e-mail basati su Web crittografati:

<<http://www.counterpane.com/crypto-gram-9908.html#Web-BasedEncryptedE-Mail>>

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

Il Canile: Cedium

Il problema è il seguente: quando qualcuno accede al vostro sito Web, può leggerne il sorgente HTML. Naturalmente non c'è modo di ovviare a questo problema: se non è possibile leggere il sorgente HTML, la pagina non può essere visualizzata. Ma encryptHTML si presenta come una possibile soluzione.

EncryptHTML è un programma che cripta pagine HTML, per poi includerle in un package munito di un programma JavaScript in grado di decodificarle. Sia le pagine codificate che il programma per decodificarle vengono inviate a chi naviga il Web, che li utilizzerà per visionare le pagine. La casa produttrice prosegue menzionando l'uso dell' algoritmo crittografico TEA, e parlando di super-sicurezza. Non vi è alcun tentativo di spiegazione di come si possa ritenere sicuro qualcosa quando si distribuisce il programma di decodifica insieme ai dati crittografati.

Il tutto diventa ancora più buffo. In Mozilla, quando si seleziona "Salva pagina con nome..." dal menu File, il browser salva semplicemente il file come testo HTML. Dato che lo script di decodifica è già stato avviato, il codice HTML è già stato decrittato.

Sicurezza. Quale sicurezza?

L'autore del programma è a conoscenza del problema, e ha smesso di lavorare al software un anno fa. È difficile dire se la compagnia che ospita la pagina Web, Cedium, ne sia al corrente. Il link per scaricare il software ha smesso di funzionare un mese fa, per cui non so che cosa stia accadendo. Questo potrebbe diventare uno dei tanti siti Web abbandonati che affollano la Rete.

Divertente, in ogni caso.

<<http://htmlcrypt.cedium.net/>>

** **

Counterpane -- un'importante ricerca

"L'implementazione di attacchi chosen-ciphertext contro PGP e GnuPG"

K. Jallad, J. Katz, e B. Schneier, Information Security Conference 2002 Proceedings, Springer-Verlag, 2002, in pubblicazione.

Si dimostra un attacco social-engineering ai danni di PGP e di altri sistemi compatibili per la crittografia di e-mail. L'attacco si svolge in questo modo:

1. Alice manda a Bob un messaggio in codice, crittografato tramite la chiave di Bob. Eve intercetta il messaggio.
2. Eve utilizza il testo cifrato intercettato per creare un messaggio criptato diverso, che poi manda a Bob.
3. Bob decodifica il messaggio. Il risultato è uno scritto inintelligibile.
4. Eve in qualche modo convince Bob a mandarle quello scritto incomprensibile.
5. Eve ricostruisce il testo originale (quello del punto 1) dal testo che riceve al punto 4.

<<http://www.counterpane.com/pgp-attack.html>>

** **

Licenza di hacking

Un nuovo progetto di legge presentato al Congresso conferisce ai detentori del copyright -- RIAA, MPAA e simili organismi -- il diritto di penetrare nei computer degli utenti nel caso abbiano fondate ragioni per credere che vi sia in atto una violazione del copyright. Essenzialmente il progetto di legge mette al sicuro queste organizzazioni dalla giustizia statale e federale nel caso disabilitino, blocchino o comunque danneggino una rete peer-to-peer accessibile pubblicamente.

Qui bisogna soffermarsi su due aspetti. Il primo è domandarsi perché la violazione del copyright necessiti di leggi speciali che autorizzino una giustizia da vigilantes (se qualcuno penetrasse nei computer di una banca e rubasse un miliardo di dollari, la banca non sarebbe legalmente autorizzata ad una ritorsione, mettendo fuori uso il computer di chi ha attaccato). Il secondo è fermarsi a considerare la natura del contrattacco.

La miglior difesa è un buon attacco, la natura del contrattacco è tutta qui. Una difesa passiva consiste nel rendersi più difficili da colpire, mentre una difesa attiva consiste nel reagire colpendo. Il contrattacco è il rovesciamento di posizioni, è attaccare l'attaccante. È in assoluto il miglior sistema per difendersi, ma è anche il più incline agli errori.

Nella quasi totalità delle società civili, il contrattacco non è legale. Se sorprendete un ladro mentre svaligia il vostro appartamento, non è legale seguirlo a casa sua e sparargli. Se qualcuno vi ricatta, reagire ricattandolo è illegale allo stesso modo. Non mi vengono in mente eccezioni a questa regola. Il rispetto della legge è l'unico scopo della polizia, un'organizzazione che possiede quel che una volta ho descritto come "un monopolio sulla violenza sponsorizzato dallo stato".

La grande eccezione a quanto sopra riportato è lo stato di guerra. In guerra le regole che riguardano il contrattacco -- e l'attacco preventivo -- sono diverse. In guerra, l'attacco e la difesa sono così confusi fra loro che il contrattacco è la

norma. In guerra, la differenza fra un'arma di attacco e una di difesa è la direzione in cui viene puntata. Ma non è di questo che stiamo parlando qui.

Il contrattacco è sbagliato, da un punto di vista legale e morale. Una giustizia da vigilantes è sbagliata, da un punto di vista legale e morale. Le vittime di un attacco hanno il diritto di difendersi, ma non è permesso loro di farsi giustizia da soli e contrattaccare. Ecco perché esiste la polizia.

Nulla di questo è una questione nuova o controversa; allora perché i detentori di copyright ne parlano? Questo progetto di legge permetterà legalmente a MPAA, RIAA e affini di penetrare all'interno di sistemi informatizzati che sospetteranno (senza avere alcuna prova concreta) essere colpevoli di violazioni del copyright. Avranno il permesso di condurre attacchi DoS ai danni di reti peer-to-peer, di diffondere virus che mettono software e sistemi fuori uso, e di violare l'altrui privacy. Le persone che verranno prese di mira saranno giudicate colpevoli fino a prova contraria. In breve, questo progetto di legge renderà l'industria dell'intrattenimento simile a una Gestapo, senza alcuna supervisione.

A mio modo di vedere, questo è l'ennesimo esempio del punto a cui le aziende dell'intrattenimento sono disposte ad arrivare per mantenere i propri modelli commerciali. Sono intenzionate a distruggere la nostra privacy, a dichiarare illegali dei comuni computer, e ad esercitare speciali poteri di polizia che nessun altro possiede... solo per assicurarsi che nessuno guardi "La Sirenetta" senza pagare. Stanno cercando di inventare un nuovo crimine: interferenza con un modello commerciale.

È molto triste, davvero.

<<http://zdnet.com.com/2100-1106-946341.html>>
<<http://www.wired.com/news/politics/0,1283,54153,00.html>>
<<http://www.newscientist.com/news/news.jsp?id=ns99992464>>

Analisi:

<<http://online.securityfocus.com/columnists/99>>

Un articolo d'opinione da parte di Howard Berman:

<<http://www.house.gov/berman/p2p062502.html>>

** **

News

Il mese scorso ho parlato di Cryptico nella mia rubrica "Il canile", sulla base di un comunicato stampa che aveva molto il sapore di un imbroglio. Pare che almeno un crittografo di tutto rispetto, Ivan Damgård, sia coinvolto in questa compagnia. Sono sempre dell'idea che si tratti di una truffa -- nulla di ciò che ho letto mi smentisce -- ma ci può essere qualcosa di un certo interesse matematico all'interno di tutte quelle stupidaggini commerciali. Hanno brevettato il loro algoritmo, comunque, e questo garantisce di sicuro la morte delle loro idee.

<<http://www.2minvest.com/news.asp?id=216>>

Un divertente aneddoto riguardante il New York Times e le password non sicure:

<<http://www.oreillynet.com/cs/weblog/view/wlg/1482>>

Qualcosa di buono arriva da Microsoft. Il suo "Five-Minute Security Advisor" è una serie di trucchi e consigli su svariati argomenti, fra cui "Semplice impostazione di un firewall per l'utenza domestica", "Guida alla protezione del portatile per il girovago informatico" e "Configurare il proprio computer per la multiutenza". C'è molta propaganda pro-Microsoft in tutto questo (un buon esempio: "come proteggere la propria privacy grazie a Windows XP"), ma vi sono anche parecchie informazioni utili.

<<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/5min/default.asp>>

Si veda anche la serie di guide "Security How-To" di Microsoft per informazioni più approfondite su determinati argomenti:

<<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/howto/sechow.asp>>

Interessanti affermazioni e controaffermazioni sul rapporto fra hacker a scopo di crimine e compagnie per la sicurezza informatica:

<<http://theregister.co.uk/content/55/26198.html>>

<<http://theregister.co.uk/content/55/26202.html>>

<<http://theregister.co.uk/content/55/26247.html>>

Per quel che può valere, non posso che nutrire rispetto per @Stake e la sua integrità in quanto azienda (faccio anche parte del loro comitato di consulenza tecnica). Non mi piacciono molto i loro rapporti con Microsoft, ma questa è un'altra cosa.

Ahi ah! Questo potrebbe diventare davvero un brevetto sui firewall di rete.

<<http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=/netacgi/srchnum.htm&r=1&f=G&l=50&s1='5.790,554'.WKU.&OS=PN/5.790,554&RS=PN/5.790,554>>

Questo mi sa parecchio di truffa. Quel che mi auguro è che il reporter si sia sbagliato e che vi sia qualcosa di interessante nelle ricerche che vi stanno sotto.

<<http://news.uns.purdue.edu/UNS/html4ever/020625.Atallah.security.html>>

Un'astuta idea per quanto riguarda la sicurezza: l'industria musicale sta invadendo le varie reti peer-to-peer di copie contraffatte di brani famosi.

<<http://www.siliconvalley.com/mld/siliconvalley/3560365.htm>>

L'American Civil Liberties Union (ACLU) sfida il DMCA:

<<http://news.com.com/2100-1023-946266.html>>

Il NIST sta cercando commenti per quanto concerne la sicurezza wireless: 802.11, Bluetooth, ecc.

<<http://csrc.nist.gov/publications/drafts.html>>

<<http://csrc.nist.gov/publications/drafts/draft-sp800-48.pdf>>

Carnival Booth è un algoritmo per sconfiggere il CAPS (Computer-Assisted Passenger Screening System). Lo scopo del CAPS è quello di cercare di massimizzare le risorse per la sicurezza stendendo profili di possibili terroristi e concentrando maggiori sforzi su di essi. "Perché perquisire Eleanor, la vecchietta ottantenne che viene dal Texas, quando si può fermare Omar, lo studente ventiduenne che arriva fresco fresco dalla Libia?" Sembra una buona teoria, ma gli autori di questo scritto dimostrano che, data una popolazione ragionevolmente mutevole di terroristi, questo sistema si rivela essere meno sicuro delle perquisizioni casuali. Davvero un buon lavoro, e un esempio eccellente di come si possano applicare al mondo reale alcune tecniche di sicurezza legate all'informatica.

<<http://swissnet.ai.mit.edu/6805/student-papers/spring02-papers/caps.htm>>

Come ci si aspettava, la rilevazione facciale automatizzata fallisce miseramente all'aeroporto Logan di Boston (i link di questo giornale sono tremendi, fra l'altro):

<http://www.boston.com/dailyglobe2/198/metro/Face_testing_at_Logan_is_found_lacking+.shtml> <http://www.boston.com/dailyglobe2/217/business/Reliability_of_face_scan_technology_in_disputeP.shtml>

Questo è un attacco che potrebbe causare seri danni: il programma MSN TV si mette a chiamare il numero di emergenza 911 dopo che un programma maligno ha cambiato le impostazioni dial-out. Tutto questo potrebbe seriamente compromettere i servizi di emergenza.

<<http://news.com.com/2100-1040-945911.html>>

Vedo che si parla sempre più spesso di contrattacco: reagire ed attaccare il computer che vi sta attaccando. Appagante finché si vuole, ma illegale in primo luogo. (come è illegale andare a svaligiare la casa di chi vi ha derubati).

<<http://online.securityfocus.com/columnists/98>>

Il Governo USA intende rendere obbligatori dei controlli di base sul personale IT?

<<http://www.computerworld.com/securitytopics/security/story/0,10801,72921,00.html>>

Eli Lilly ha dovuto rispondere davanti al Governo USA di un caso di responsabilità legata alla privacy. Avevano diffuso i nominativi di 669 pazienti in cura con il Prozac.

<<http://www.computerworld.com/securitytopics/security/privacy/story/0,10801,72978,00.html>>

Nuovo risultato critto-analitico Rijndael. Non si tratta di un attacco, ma di una proprietà matematica dell'algoritmo recentemente scoperta che potrebbe portare a un attacco.

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

Un nuovo e più veloce algoritmo per verificare che un dato numero sia un numero primo o no. Se da un lato questo non presenta implicazioni crittografiche, dall'altro si tratta di un grosso passo avanti. Infatti la possibile esistenza di un simile algoritmo era stata una questione aperta finora.

<<http://www.cse.iitk.ac.in/news/primality.pdf>>

Vi è un'enorme falla nella sicurezza SSL di Microsoft Internet Explorer. Chiunque dotato di un valido certificato VeriSign per un qualsiasi sito Internet può creare un certificato falso per ogni altro sito Internet, e Microsoft Internet Explorer prenderà come valido anche il certificato falso. Lo standard X.509 specifica che i certificati devono includere un bit che indichi se la corrispondente chiave pubblica possa venire adoperata per firmare altri certificati. I certificati VeriSign, naturalmente, hanno quel bit disabilitato. Ma Microsoft IE non controlla il bit e crede che ogni certificato possa firmare qualsiasi altro certificato, e che ogni certificato così firmato sia valido. Questo significa che se siete un utente di IE, le protezioni crittografiche in SSL non vi funzioneranno. Il fatto che Microsoft non sembri molto interessata a questo problema mi fa capire come la loro iniziativa di "prendere sul serio la sicurezza" sia in gran parte aria fritta.

<<http://www.theregus.com/content/4/25935.html>>

<<http://www.eweek.com/article2/0,3959,462375,00.asp>>

<http://story.news.yahoo.com/news?tmpl=story&u=/ap/20020812/ap_on_hi_te/encryption_flaw_2>

** ** ** ** **

Le news di Counterpane

Bruce Schneier è il soggetto di un lungo ed assai interessante articolo sul The Atlantic:

<<http://www.theatlantic.com/issues/2002/09/mann.htm>>

Per Counterpane è stato il miglior trimestre in assoluto. Stiamo monitorando sempre più compagnie in sempre più paesi, e siamo ormai la più grande azienda di monitoraggio della sicurezza a livello mondiale. In più, con l'assorbimento di RipTech da parte di Symantec, non esiste nessun'altra compagnia di monitoraggio della sicurezza che possa vantarsi di essere indipendente dai rivenditori. Ormai abbiamo più di 70 rivenditori che offrono i servizi di monitoraggio di Counterpane, e il numero cresce di settimana in settimana. È davvero fantastico.

Il secondo trimestre di Counterpane:

<<http://www.counterpane.com/pr-2002q2.html>>

** ** ** ** **

Armare i piloti delle linee aeree

È una soluzione essenzialmente americana: le linee aeree commerciali nazionali sono a rischio. Allora perché non permettere ai piloti di essere armati? Abbiamo davanti agli occhi le immagini di questi baldi uomini e donne, l'ultima linea di difesa su un aeroplano, che difendono coraggiosamente la cabina di pilotaggio contro i terroristi, a 30.000 piedi di altitudine. Già m'immagino i vari TV movie.

La realtà è assai più complicata della televisione, però. A volte i sistemi di sicurezza causano più problemi di quanti dovrebbero risolverne. Mettere delle armi su un aereo ci renderà più vulnerabili agli attacchi, e non il contrario.

Quando la gente pensa ai potenziali problemi legati alla presenza di armi in una cabina di pilotaggio, in genere pensa a colpi sparati accidentalmente in aria, fori nella fusoliera, e magari una parte delle apparecchiature distrutta da una pallottola vagante. Questi sono indubbiamente dei problemi, certo, ma non i principali. Il foro di una pallottola non è molto grande, e non fa fuoriuscire molta aria. Gli aerei sono progettati per gestire dei guasti alle apparecchiature, anche seri, e rimanere ugualmente in volo. Se possedessi una compagnia aerea sarei più preoccupato di incidenti riguardanti i passeggeri, che sono di certo più vulnerabili alle ferite da arma da fuoco, e che possono sporgere denunce.

I pericoli reali, quindi, riguardano i complessi sistemi che devono essere preparati prima che compaia la prima arma all'interno di una cabina di pilotaggio. Vi sono grandi aree di rischio.

Primo: occorre un modo per far arrivare l'arma sull'aereo. Come dare una pistola al pilota? La porta con sé in aeroporto e poi sull'aereo? Gli viene consegnata non appena egli si trova in cabina ma prima che l'aereo decolli? Viene posta in un luogo sicuro nella cabina sempre e comunque, anche quando non vi è nessuno? Ognuna di queste soluzioni presenta una propria serie di vulnerabilità a livello di sicurezza. L'ultima cosa che vogliamo è che un malintenzionato sfrutti queste debolezze per procurarsi l'arma. O forse l'ultima cosa che vogliamo è una sparatoria nel bel mezzo di un aeroporto affollato.

Secondo: occorre una procedura per collocare l'arma sull'aereo. Il pilota la porta sempre al fianco? È chiusa in un contenitore? In questo caso chi ne possiede la chiave? Vi è un'unica arma, oppure il pilota e il co-pilota ne possiedono una per ciascuno? Comunque funzioni questo sistema, è facile abusarne. Se la pistola è al fianco del pilota, un malintenzionato può sottrargliela quando abbandona la cabina (non ridete: ai poliziotti vengono sottratte in continuazione, e sono istruiti per evitarlo). Se le pistole rimangono in cabina quando non c'è nessuno, allora ci troviamo di fronte a tutta una nuova serie di problemi.

Terzo: occorre un sistema per istruire i piloti a maneggiare e a tirare con la pistola. Le armi da fuoco richiedono molta pratica per essere utilizzate a dovere; quanta di questa pratica ci aspettiamo dai piloti? È molto diverso dall'istruire ufficiali dell'aviazione: per loro la sicurezza è il compito principale. Da loro ci si aspetta che sappiano usare un'arma. Il compito principale di un pilota è di pilotare un aereo.

Armare i piloti è l'anticamera di un disastro. Le disposizioni attuali spendono parecchio tempo ed energie per tenere lontane le armi dagli aerei e dagli aeroporti; lo schema proposto introdurrebbe migliaia di rivoltelle. Vi sono troppi piloti e troppi voli quotidiani, e accadranno di sicuro degli errori. Dopo un inventario notturno si potrebbe scoprire che manca una pistola, o dieci. Qualcuno ne troverà una abbandonata in una cabina di pilotaggio. Qualcun altro potrebbe anche trovarne una abbandonata su un sedile in un terminal.

El Al è la compagnia aerea più attenta alla sicurezza in tutto il mondo. I suoi piloti sono protetti da due sportelli antiproiettile, e sono disarmati. È compito del pilota far atterrare l'aereo in modo sicuro, non certo affrontare i terroristi in un combattimento corpo a corpo. Per quello si affidano ad ufficiali militari, all'equipaggio, ai passeggeri. Se i piloti devono abbandonare la cabina di pilotaggio per risolvere un problema di sicurezza, allora è troppo tardi.

Le compagnie aeree statunitensi non sono paragonabili alla El Al. I nostri voli non viaggiano con due ufficiali armati. Non si effettuano controlli di sicurezza sui passeggeri che -- pur essendo legali in Israele -- violerebbero le leggi americane. Non abbiamo due sportelli antiproiettile che separano la cabina dai passeggeri. Molti politici vedono le pistole come una rapida soluzione a un problema che non può aspettare una soluzione più ragionata.

Personalmente non credo che i piloti dovrebbero essere armati. Ma anche se pensassi il contrario, non li armerei lo stesso. Le pistole non sono fatte per gli spazi angusti di una cabina di pilotaggio. Il rischio di causare danni accidentali è troppo alto. Come è alto il rischio di introdurre migliaia di pistole negli aeroporti, di sistemarle, di trasportarle su e giù dagli aerei, di conservarle in cabina. Se si vogliono armare i piloti, avrebbe più senso dotarli di manganelli o di taser (un immobilizzatore, ndt). Se non altro, sono armi più appropriate al contesto.

** ** ** ** **

Commenti dei lettori

Da: Travis Puderbaugh <tpuderbaugh@amada.com>

Oggetto: Sistemi embedded

