





anche sulla vulnerabilità stessa, e questo potrebbe risultare in una violazione del DMCA. Ridicolo? Certo che lo è, ma questa è la legge...

<<http://www.theregus.com/content/4/26656.html>>

Dato che siamo in tema di cose ridicole, ecco alcuni dei "dispositivi digitali" che dovrebbero obbligatoriamente incorporare la tecnologia anti-copia approvata dal governo mediante l'Hollings CBDTPA Bill: apparecchi acustici, portaritratti parlanti, cartelli scorrevoli e baby monitor.

<[http://www.freedom-to-tinker.com/archives/cat\\_fritzs\\_hit\\_list.html](http://www.freedom-to-tinker.com/archives/cat_fritzs_hit_list.html)>

Questi sono due esempi del tipo di cose che accadono quando le leggi vengono scritte per proteggere i profitti di un'industria senza tener conto degli effetti che hanno sull'intera società. Un altro esempio sono le estensioni alle leggi sul copyright, che attualmente sono in fase di discussione alla Corte Suprema. Qui si possono trovare alcune riflessioni di Larry Lessig riguardanti questo dibattito:

<[http://cyberlaw.stanford.edu/lessig/blog/archives/2002\\_10.shtml#000531](http://cyberlaw.stanford.edu/lessig/blog/archives/2002_10.shtml#000531)>

Un reporter in gamba dell'agenzia Reuters indovina l'URL dei profitti del terzo trimestre di un'azienda svedese (prima che questi fossero "ufficialmente" pubblicati). L'azienda dichiara che intraprenderà azioni legali. È una domanda interessante: indovinare un URL è una "intrusione"? Non credo.

<<http://www.theregister.co.uk/content/6/27816.html>>

<<http://salon.com/tech/wire/2002/10/28/reuters/index.html>>

Il Security Business Quarterly è una pubblicazione che merita di essere letta. I numeri sono disponibili on-line.

<<http://www.s bq.com>>

Windows 2000 ha ricevuto una graduazione di affidabilità in base ai Common Criteria per la sicurezza. Questo vuol forse dire qualcosa? Non proprio. Jonathan Shapiro ha spiegato i motivi in maniera così brillante che segnalo il link del suo intervento:

<<http://eros.cs.jhu.edu/~shap/NT-EAL4.html>>

Chi utilizza prodotti Microsoft potrebbe dover pagare per ottenere sicurezza. In effetti ritengo che non sia una cattiva idea. Se gli utenti sono intenzionati a pagare la sicurezza, allora ci sono maggiori possibilità che Microsoft sia ritenuta responsabile di quella sicurezza. In tutta onestà, a moltissimi utenti non importa la sicurezza e non hanno intenzione di pagarla.

<<http://www.zdnet.it/zdnet/JumpNews.asp?idChannel=837&idNews=158149>>

<<http://zdnet.com.com/2100-1104-961173.html>>

Questo articolo dice: "La rete del terrore di al-Qaeda ha incominciato a servirsi di hacker che penetrano nei siti Web per creare pagine segrete che inviano messaggi ai suoi seguaci, sostengono alcuni specialisti di Internet". Tutto ciò non ha alcun senso, ed è un triste esempio del genere di sensazionalismo legato alla sicurezza informatica che rivela soltanto un cieco antiterrorismo, e che purtroppo è molto frequente in questo periodo.

<<http://cooltech.iafrica.com/technews/179588.htm>>

Un'analisi ottimamente scritta in merito alle problematiche di Windows XP legate alla sicurezza, alla privacy e alla stabilità.

<<http://www.hevanet.com/peace/microsoft.htm>>

"Lo scorso anno le aziende che fanno parte di Fortune 1000 hanno perso 45 miliardi di dollari in seguito a furti di informazioni proprietarie." Come fanno a saperlo?

<[http://www.infoworld.com/suppsad/ISS/t\\_issprt1.html](http://www.infoworld.com/suppsad/ISS/t_issprt1.html)>

"Valutare i rischi della sicurezza informatica" (Assessing Internet Security Risk), in cinque parti:

<<http://online.securityfocus.com/infocus/1591>>  
<<http://online.securityfocus.com/infocus/1607>>  
<<http://online.securityfocus.com/infocus/1612>>  
<<http://online.securityfocus.com/infocus/1631>>  
<<http://online.securityfocus.com/infocus/1632>>

Server root DNS attaccati. Bisogna ringraziare i "buoni" se le conseguenze dell'attacco sono state di lieve entità. Se ne parla molto, tuttavia.

<<http://www.washingtonpost.com/wp-dyn/articles/A828-2002Oct22.html>>  
<<http://www.newsfactor.com/perl/story/19756.html>>  
<<http://www.cnn.com/2002/TECH/internet/10/23/net.attack/index.html>>  
<<http://www.zdnet.it/zdnet/JumpNews.asp?idChannel=837&idNews=158150>>  
<<http://www.zdnet.it/zdnet/JumpNews.asp?idChannel=837&idNews=158151>>  
<<http://computerworld.com/newsletter/0%2C4902%2C75350%2C0.html?nlid=SEC>>  
<<http://www.esj.com/news/article.asp?EditorialsID=317>>  
<<http://www.eweek.com/article2/0,3959,651686,00.asp>>

Una storia di sicurezza informatica a lieto fine: la NASA.

<<http://www.infoworld.com/articles/op/xml/02/10/28/021028opsecurity.xml>>  
<<http://www.fcw.com/fcw/articles/2002/1014/mgt-nasa-10-14-02.asp>>

Lo United States Copyright Office invita il pubblico al dibattito sul DMCA:

<<http://www.zdnet.it/zdnet/JumpNews.asp?idChannel=837&idNews=158153>>  
<<http://www.copyright.gov/1201/>>

Un'affascinante deposizione congressuale da parte del direttore della NSA, Michael Hayden. Egli spiega come la NSA si sia occupata del terrorismo precedente e seguente l'11 settembre, poi dice al governo che potrebbe essergli molto più utile se si rivolgesse agli elettori e cercasse di individuare dove l'opinione pubblica sia disposta a tracciare la linea di confine fra libertà e sicurezza. Lettura obbligatoria.

<<http://intelligence.senate.gov/0210hrg/021017/hayden.pdf>>

Eccellente intervento di Carl Ellison sulle leggende e le realtà della PKI:

<<http://www.cs.dartmouth.edu/~pki02/Ellison/>>

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

Le news di Counterpane

Vi sono parecchie grosse novità di cui non posso ancora parlare. I dettagli, se tutto va bene, nel prossimo numero.

Nel frattempo interverrò al COMDEX a Las Vegas il 18 novembre, all'incontro della IETF ad Atlanta il 22 novembre e all'InfoSecurity a New York l'11 dicembre.

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

Note di sicurezza da ogni dove: le api giapponesi

I calabroni attaccano sistematicamente gli alveari. In genere, un attacco ha inizio quando un calabrone cattura un'ape solitaria nei pressi dell'arnia. Dopo una serie ripetuta di queste schermaglie esterne, un calabrone rilascia un ferormone "marcatore" all'ingresso dell'alveare. Questo ferormone attrae gli altri calabroni, che arrivano in massa per attaccare l'alveare. I pungiglioni delle api non sono in grado di penetrare la corazza dei calabroni, per cui è una lotta impari; qualcosa come 30 mila api possono venire uccise in poche ore da 30-40 calabroni.



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

## Commenti dei Lettori

Da: Frank Prince <[fwp3@grumpybear.com](mailto:fwp3@grumpybear.com)>

Oggetto: La strategia nazionale per rendere sicuro il Cyberspazio

Non sono d'accordo sul fatto che la strategia non faccia differenza. Ritengo che i suoi commenti siano stati troppo conclusivi a riguardo.

C'era qualcosa che non mi quadrava nella discussione sul rapporto fra il consenso unanime e la sicurezza. In riferimento alla sicurezza, il consenso -- in una comunità, in un'assemblea, formalizzato in legge, o segnato da un precedente legale -- è una sorta di stima della minaccia ai beni comuni e di decisione di ripartizione delle risorse. Possiamo indubbiamente affermare che sia imperfetto, ma non che sia irrilevante.

Inoltre non sono d'accordo con l'idea secondo cui la sicurezza è un bene comune. Le nuove risorse comunitarie che stiamo cercando di proteggere non sono completamente definite. Il consenso riguardante ciò che minaccia queste risorse rimarrà inconsistente finché esse non saranno definite. In più, i parametri che ci permetteranno di stabilire le responsabilità sono ancor meno stimabili. La sicurezza, così come la disponibilità, è un elemento che può venire usato come metro di giudizio quando il bene comune è in crisi. Ma ciò che sta alla base del problema non è la sicurezza, ma l'adattamento culturale verso realtà tecnologiche capaci di profondi cambiamenti.

Detto questo, in qualsiasi momento storico di grandi cambiamenti vi sono sempre stati dei criminali che hanno approfittato dello scompiglio. Non possiamo permettere a questi individui di danneggiarci. Allo stesso tempo dobbiamo ricordare che siamo impegnati in una lotta che avviene su due piani temporali differenti -- il primo riguarda le nostre decisioni quotidiane in merito alla sicurezza, e il secondo riguarda la nostra comprensione nel lungo periodo degli effetti che avrà sulla sicurezza il cambiamento tecnologico. Il quotidiano interagisce con il lungo periodo. Una nuova tecnica per ridurre l'impatto degli attacchi di tipo denial-of-service cambia la percezione che la gente ha della loro gravità. Il medesimo effetto viene prodotto dal "pallone-sonda" che il governo lancia in merito alla cyber-sicurezza, che va ad influenzare i finanziamenti per la ricerca così come la consapevolezza dell'opinione pubblica. Entrambe le cose fanno differenza. Nessuna delle due è irrilevante.

Da: "Odom, Joel" <[Joel.Odom@BellSouth.com](mailto:Joel.Odom@BellSouth.com)>

Oggetto: La strategia nazionale per rendere sicuro il Cyberspazio

Nella stessa misura in cui la "strategia nazionale per rendere sicuro il Cyberspazio" non farà nulla per migliorare la sicurezza informatica, l'approvare leggi che impongono certi comportamenti di sicurezza, alle aziende così come ai privati, sarà altrettanto deleterio.

Come lei ha affermato, il governo è soltanto politica e non si cura di ciò che sarà in grado di funzionare. Le leggi sulla sicurezza informatica richiederanno delle procedure che renderanno i sistemi ancora più complicati. Quando un sistema diviene più complicato, solitamente finisce con l'essere meno sicuro, non più sicuro.

Le leggi non sarebbero in grado di ordinare l'investigazione e il responso necessari per una vera sicurezza. Al contrario, ordinerebbero la fiducia su determinati prodotti e soffocherebbero tutti gli sforzi che vengono fatti in buona fede per migliorare la sicurezza. Ancora peggio, infonderebbero agli utenti una falsa sensazione di sicurezza.

Il modo migliore per danneggiare la sicurezza informatica è lasciare che il governo vi metta mano. Tutte le leggi sulla sicurezza che sono state approvate negli ultimi anni non hanno fatto

altro che peggiorare le cose. Non capisco perché ci aspettiamo che il governo possa davvero risolvere il problema...

A: Bruce Schneier <[schneier@counterpane.com](mailto:schneier@counterpane.com)>

Oggetto: La strategia nazionale per rendere sicuro il Cyberspazio

"La sicurezza è un bene comune. Come l'aria, l'acqua e le onde radio, l'uso individuale influisce sulla collettività. Il modo per evitare che le persone abusino di un bene comune è quello di regolamentarlo. Se le aziende hanno smesso di gettare rifiuti tossici nei fiumi, è perché il governo ha usato le maniere forti, e non i guanti bianchi. Le aziende hanno smesso perché quella pratica è stata resa illegale."

No. Il modo per evitare che le persone abusino di un bene comune è quello di stabilire e far rispettare i diritti di proprietà. Una toilette pubblica sarà sempre sporca a prescindere da quante leggi vengano approvate. Molte aziende rispettano le leggi contro lo scarico abusivo dei rifiuti, ma ve ne sono molte altre che sono semplicemente diventate più creative sul dove e quando inquinare. Le leggi non funzionano. Abbiamo bisogno di persone che abbiano interesse a proteggere la loro proprietà, non burocrati che proteggeranno i beni comuni fino a quando qualcuno non li convincerà a fare l'opposto corrompendoli, e non governi che emanano leggi ma si rendono automaticamente dispensati.

La parte difficile è distribuire i beni comuni in "parti" omogenei di proprietà, per assicurare che il maggior numero di persone possa ancora utilizzarli ad un prezzo equo.

Da: Marc de Piolenc <[piolenc@mozcom.com](mailto:piolenc@mozcom.com)>

Oggetto: La strategia nazionale per rendere sicuro il Cyberspazio

Se da un lato sono d'accordo con lei sull'inefficacia di un progetto senza mordente, dall'altro ho i miei dubbi sull'efficacia della legislazione. La sua analogia con le disposizioni antinquinamento è valida, poiché mette in luce la credenza erronea in un "bene comune".

Ciò che appartiene a tutti non appartiene a nessuno, nel senso che nessuno è incentivato a preservarlo. La risposta non dev'essere quella di dare poteri ai burocrati per proteggere i beni comuni (cosa che farebbero male o non farebbero del tutto), ma di privatizzare le risorse che vengono comunemente gestite come dominio pubblico.

Nel caso dell'infrastruttura di cui stiamo parlando, essa si trova già in mano ai privati, e considerarla un "bene comune" è soltanto un modo stravagante di permettere a coloro che ne controllano le varie parti di sfuggire alle responsabilità legate a questa gestione.

Per fare un semplice esempio, i proprietari di reti di distribuzione sono -- negli USA almeno -- perseguibili civilmente in caso di mancato adempimento delle regole stabilite di buona pratica nei loro rispettivi ambiti tecnici. Qui non è questione di regolamentazione, ma di legge sugli illeciti civili. Il problema del nostro settore è l'assenza di regole di buona pratica unanimemente riconosciute. Un qualsiasi passo avanti in questa direzione vale ogni tonnellata di scartoffie emanate dal Federal Register (la Gazzetta Ufficiale statunitense, ndt).

Da: Jim Reid <[jim@rfc1035.com](mailto:jim@rfc1035.com)>

Oggetto: La strategia nazionale per rendere sicuro il Cyberspazio

Credo che i suoi commenti riguardanti il consenso unanime in un'ottica di questioni di sicurezza avrebbero potuto essere espressi con maggiore accortezza. La sicurezza, in definitiva, riguarda il consenso. Deve essere un bilanciamento fra ciò che gli utenti finali potranno tollerare, ciò che potrà tollerare chi si occupa di sicurezza, ciò che i vari provider sono disposti ad offrire in termini di servizi, e ciò che i vari ragionieri accetteranno in quanto a costi e rischi/compensi. Se questi conflitti d'interesse riusciranno ad essere adeguatamente bilanciati, allora il sistema che ne risulterà sarà abbastanza sicuro per gli scopi prefissati originariamente. È piuttosto

ingiusto da parte sua affermare che la sicurezza consensuale spesso finisce col diventare una serie di cattive decisioni. In una società libera ritengo che sia impossibile predisporre sistemi di sicurezza concreti, se questi sistemi non vengono costruiti intorno al consenso.

Dove mi trova completamente d'accordo con lei è quando afferma che la sicurezza -- o qualsiasi altra cosa cerchiamo di ottenere -- si inquina nel momento in cui le parti in causa si mettono a spadroneggiare o mostrano di avere un ordine del giorno ben chiaro al fine di proteggere i loro interessi acquisiti. Finiscono col distorcere il processo decisionale in modo che rifletta la loro posizione.

Da: Anonimo

Oggetto: La strategia nazionale per rendere sicuro il Cyberspazio

La sua risposta alla strategia per la cyber-sicurezza è un appello appassionato, ma non riesco a credere come lei sia giunto alle sue conclusioni. Quale legge dovrebbe emanare il governo? Dopo l'esempio del DMCA, approveranno una legge contro l'hacking o qualsiasi cosa gli assomigli, e quella legge avrà l'effetto collaterale di rendere tutta la gestione dei network (specialmente la sicurezza guidata come quella che Counterpane produce) un'attività illecita.

Le persone che lei descrive, spinte da interessi particolari ad agire in maniera debole e confusa malgrado tutta la mole di buoni consigli, premeranno il grilletto -- ma cosa andranno a colpire?

Dunque, quale legge vorrebbe che fosse emanata? Pare proprio che lei voglia una sola legge: che renda le aziende perseguibili in caso di attacchi andati a buon fine. Counterpane, sarebbe perseguibile?

Sospetto che lei voglia che sia Microsoft ad essere resa perseguibile -- come punizione per aver creato falle di sicurezza. Ma lei non lo dice. Perché si aspetta che il governo segua la stessa logica che lei ed io seguiamo? Se lei vuole che il governo renda qualcuno perseguibile, si potrebbe arrivare a rendere perseguibile un proprietario di casa perché il suo home computer è stato utilizzato come rampa di lancio per attacchi DoS -- e Microsoft non verrebbe nemmeno toccata.

Da: Stefan Lucks <[lucks@weisskugel.informatik.uni-mannheim.de](mailto:lucks@weisskugel.informatik.uni-mannheim.de)>

Oggetto: Gli attacchi XSL contro AES

Io stesso ho studiato la tecnica di risoluzione delle equazioni per la crittoanalisi di algoritmi a chiave segreta, del tipo di AES. In qualità di scienziato, trovo questa tecnica molto affascinante. Tuttavia credo sia troppo presto per arrivare a delle conclusioni.

Come ho detto, lo studio di Courtois e Pieprzyk è davvero interessante per me. La loro tecnica potrebbe rivelarsi un serio attacco ai danni di alcuni algoritmi a chiave segreta, senza escludere lo stesso AES. Ma al momento lo studio di questi algoritmi è una costante ricerca, né più, né meno. È davvero troppo presto per considerare violato AES. Si dovrebbero attendere molti altri esiti. (Non scrivo questo per criticare gli autori: hanno fatto un ottimo lavoro. Ma una buona ricerca ha bisogno di tempo e i ricercatori devono pubblicare i loro "work in progress" per avere un riscontro dai loro pari.)

In generale, la tecnica funziona in questo modo:

1. Trovare uno speciale "trucco" per descrivere l'algoritmo come un sistema di equazioni quadratiche (o di basso grado) in larga misura sovradeterminato (per crittosistemi a chiave segreta tipicamente in  $GF(2)$ ).
2. Controllare che non vi siano ovvie ragioni per cui XL non possa essere in grado di risolvere il sistema (per esempio, un eccesso di dipendenze lineari).

3. Utilizzare XL (o una sua variante) per risolvere il sistema, e incrociare le dita. Ovvero, aumentare artificialmente il numero delle equazioni moltiplicando alcune equazioni con altri termini per ottenere un sistema di equazioni non lineari (di grado superiore). Se il numero delle equazioni eccede il numero dei termini, linearizzare il sistema -- per esempio trattando ogni termine come una variabile lineare indipendente.

4. Risolvere questo (enorme) sistema di equazioni lineari.

Il problema sta nel passare dal punto 2 al punto 3. Courtois e Pieprzyk, nella loro documentazione, descrivono alcune condizioni necessarie affinché XL funzioni. Possiamo controllare queste condizioni al punto 2. Ma tali condizioni sono ben lungi dall'essere sufficienti. Soprattutto nel caso di AES rimangono forti dubbi.

Vi sono alcune indicazioni sperimentali secondo cui XL funziona almeno qualche volta. Purtroppo a tutt'oggi gli attacchi "veri" sono troppo costosi per essere implementati, per cui non possiamo verificare l'attacco direttamente.

I buoni algoritmi crittografici sono come il buon vino: hanno bisogno di tempo per maturare bene. AES è ancora giovane, ha solo cinque anni, e non avrei nulla da obiettare nel caso si ritenessero i triple DES a tre chiavi una possibile alternativa ad AES per i prossimi cinque anni o giù di lì.

Da: Ulrich Kunitz <[ulrich.kunitz@freenet.de](mailto:ulrich.kunitz@freenet.de)>  
Oggetto: One-Time pad: esempi dal mondo reale

Ho visto one-time pad usati dall'esercito dell'ex Germania Est, io stesso ho eseguito qualche cifratura, non proprio secondo le regole. Sono stato soldato semplice dal 1987 al 1989 in una base missilistica terra-aria dotata di vecchi missili Voichov SA-2. Messaggi brevi contenenti il piano delle frequenze per la rilevazione di alleati, la codifica del sistema di coordinate e dei movimenti delle truppe venivano cifrati mediante one-time pad. La cifratura e la decodifica dovevano essere fatte dagli ufficiali, come mi spiegò uno di loro. I blocchi venivano numerati e archiviati in contenitori speciali sigillati e fissati nei muri del bunker principale. Lo scambio delle chiavi era compito di corrieri armati (due uomini) muniti di una valigetta sigillata. Tutti coloro che erano a conoscenza del sistema sapevano che i blocchi di codice non dovevano essere riutilizzati. Ma si trattava ancora di un esercito tedesco con tradizioni prussiane, che contava ogni pallottola due volte. Che i russi all'ambasciata sovietica non abbiano fatto la cosa giusta può derivare dalla loro mentalità: aggirare gli ostacoli per arrivare al traguardo.

Qui in Germania, le banche utilizzano one-time pad per l'autenticazione di ordini finanziari. Questo sistema viene usato da milioni di clienti, anche da mia madre. Viene chiamato il sistema PIN/TAN. I blocchi TAN sono spediti dal servizio postale; alcune banche richiedono persino che il cliente notifichi la ricevuta con una lettera firmata. Per ogni ordine eseguito attraverso il proprio browser o un software di home banking, è necessario usare un numero di transazione (TAN) del blocco. Il sistema bancario controlla il TAN e fa rispettare l'utilizzo singolo. Lo schema non impedisce ai malintenzionati di cambiare il messaggio prima che sia spedito mediante la connessione criptata, ma limita in modo efficace la quantità di ordini che un malintenzionato può inviare, a meno che il cliente non archivi i propri TAN sul computer. Limitando la quantità di denaro per ogni ordine, il sistema riduce i rischi dal lato della banca.

Ho implementato qui in Germania diversi sistemi di banking on-line, utilizzando diversi sistemi crittografici con chiavi in un file, token e smart card. Algoritmi standard, nessuna presa in giro, conosciamo i nostri limiti. Continua a sorprendermi la facilità di apprendimento, la semplicità di applicazione (nessun driver o dispositivi aggiunti) e la relativa sicurezza del metodo PIN/TAN. Limitando il numero di ordini che un malintenzionato può fare è molto più difficile con la tecnologia disponibile a livello di smart card o di chiavi in un file. I clienti non hanno problemi a sviluppare il modello corretto riguardante il PIN/TAN, ma le smart card non fanno quel che molta gente crede che facciano.

