

ndt) hanno pubblicato documenti inerenti alla cyber-sicurezza. Ma i piani, a prescindere da quanto siano dettagliati o accurati, non rendono sicuro un bel niente; agire, invece, sì.

Nemmeno il consenso unanime rende sicuro alcunché. Le versioni preliminari del progetto usavano parole forti per quanto concerne la mancanza di sicurezza delle reti wireless, parole che sono state poi omesse perché l'industria wireless non voleva essere messa in cattiva luce per il mancato impegno in materia di sicurezza. Le versioni preliminari comprendevano il suggerimento secondo cui tutti i provider Internet avrebbero dovuto fornire dei firewall personali ai propri clienti; suggerimento eliminato perché i provider non volevano apparire negligenti per non aver già provveduto ad una cosa del genere.

E così via. Questo è ciò che si ottiene con un documento di pubbliche relazioni. Si ricevono moltissimi input dalle più svariate fonti, tutte con i propri interessi, e si finisce con l'avere un documento che non da fastidio a nessuno perché non impone nulla di particolare.

Quel che è peggio è che alcune delle persone coinvolte nella scrittura del documento erano potenti e convinti professionisti della sicurezza. Dev'essere stato un brutto risveglio per loro quando hanno capito come vanno le cose a Washington. Gli sforzi e le energie impiegati nella stesura di questo documento sono evidenti, e il fatto che esso sia stato ridotto all'essenziale a causa di interessi particolari è vergognoso... ma tipico.

Così adesso tutti si sentono a posto per aver fatto la loro parte in merito alla sicurezza, e ogni cosa rimane invariata.

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.

Nel suo intervento in merito a questo argomento, Marcus Ranum ha messo in evidenza come il consenso unanime e gli accordi non funzionino nel pianificare la sicurezza. La sicurezza sulla base del consenso porta a volte ad operare buone decisioni, ma più spesso a pessime scelte. Di per sé il consenso unanime non è dannoso; lo sono invece quasi sempre i compromessi, perché più parti sono coinvolte nella discussione, maggiori saranno i conflitti d'interesse che andranno ad ostacolare la sicurezza. Il consenso non funziona perché la parte in causa più importante di questi negoziati – chi compie un attacco - non è seduta con gli altri al tavolo delle trattative. “Gli hacker non verrebbero a patti comunque. In altre parole, raggiungere l'unanimità non serve a nulla...che essa funzioni o meno dipende da un altro insieme di regole, sulle quali le vostre richieste non esercitano alcun controllo”.

Se il governo degli Stati Uniti vuole ottenere qualcosa, dovrebbe varare una legge. È questo ciò che fanno i governi. È come con l'inquinamento: non si impongono specifiche tecnologie, ma si obbligano determinati risultati. Si ritengono responsabili le aziende per eventuali insicurezze, e ci si sorprenderà nel vedere quanto rapidamente le cose diventeranno sicure. Si lascino le rassicuranti attività di pubbliche relazioni alle varie organizzazioni industriali del settore, è ciò che ci aspetta da loro.

Il documento provvisorio:

<<http://www.whitehouse.gov/pcipb/>>

I vari articoli che annunciano la notizia:

<http://www.bangkokpost.com/021002_Database/02Oct2002_dbcol10.html>

<<http://www.infoworld.com/articles/hn/xml/02/09/>

[18/020918hnnatcyber.xml?s=IDGNS](http://www.infoworld.com/articles/hn/xml/02/09/18/020918hnnatcyber.xml?s=IDGNS)>

<<http://www.computerworld.com/securitytopics/security/story/0,10801,74449,00.html>>

Il mio scritto su XLS nello scorso numero di Crypto-Gram:
<<http://www.cryptogram.it/settembre02.htm#a1>>

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

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.

Cyber-terrorismo:
<<http://www.cryptogram.it/ottobre.html#Articolo1>>

I pericoli della porta 80:
<<http://www.cryptogram.it/ottobre.html#Articolo9>>

Attacchi semantici:
<<http://www.counterpane.com/crypto-gram-0010.html#1>>

La NSA sulla sicurezza:
<<http://www.counterpane.com/crypto-gram-0010.html#7>>

"Così vorresti diventare un crittografo":
<<http://www.counterpane.com/crypto-gram-9910.html#SoYouWanttobeaCryptographer>>

Lunghezza delle chiavi e sicurezza:
<<http://www.counterpane.com/crypto-gram-9910.html#KeyLengthandSecurity>>

Steganografia: verità e fantasie:
<<http://www.counterpane.com/crypto-gram-9810.html#steganography>>

Appunti per gli apprendisti scrittori di algoritmi crittografici:
<<http://www.counterpane.com/crypto-gram-9810.html#cipherdesign>>

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

Il Canile: GreatEncryption

Questo presenta tutti gli ingredienti del classico software-truffa: un nuovo algoritmo crittografico che non viene discusso, una palese ignoranza in materia di crittografia, un brevetto ancora da approvare, e una finta competizione. Alcune frasi di esempio prese dal sito web: "Chiavi lunghe dai 2000 ai 4000 caratteri sono consigliate per una chiave di gran lunga più forte di ogni altro software finora prodotto" "Un software con forza di chiave $109^{4000} + 109^{3999} + \dots + 109^1$ ". Caspita.

La parte più divertente è quando dichiarano quanto è veloce la loro crittografia, che "codifica circa 5000 caratteri al secondo di testo in chiaro su un PC di medie prestazioni". Ammettiamo che un PC di medie prestazioni viaggi a 500 MHz; questo significa circa 100.000 cicli di clock per byte (carattere ASCII) codificato. AES codifica a 20 cicli di clock per byte; esistono stream cipher veloci più del doppio. Ciò vuol dire che AES è 5000 volte più veloce di GreatEncryption.

Da: "Christian Hampson" <champson@hampsonservices.com>

Oggetto: Il suo nome nell'elenco di Reveal

Per quanto riguarda l'inclusione del suo nome e di quello del Rabbino Schneerson sull'elenco per Reveal, il termine "cripta" viene considerato parola occulta. Il suo nome è strettamente connesso con la crittografia. Inoltre, Avi Schneier viene connesso con il Tai Chi a New York, e Arthur Schneier fa parte dell'International Center for Religion and Diplomacy. Come per Schneerson, ho anche notato come siano considerate occulte parole quali "giudeo", "Hasidi" e "Cabala". Pare che qualsiasi cosa al di fuori della Religione Civile sia da considerarsi occulto, dato che "Allah", "canto", "Mahayana", "Sabat", "rituale", "profeta" e "risurrezione" sono tutti termini inclusi nella lista. Forse dovrebbe sentirsi onorato per questa inclusione.

Da: Douglas Davidson <drd@alumni.princeton.edu>

Oggetto: Il suo nome nell'elenco di Reveal

Intendevo soltanto evidenziare come ciò possa non essere necessariamente illegittimo. Se questa organizzazione fa uso di un qualche tipo di filtro statistico (qualcosa di analogo a quanto descritto su <<http://www.paulgraham.com/spam.html>> in merito ai filtri per lo spam), allora è del tutto plausibile che il loro elenco di parole sia derivato interamente e automaticamente dall'analisi di qualche corpus (raccolta di informazioni, ndt). In questo caso, la presenza di una certa parola potrebbe essere piuttosto difficile da spiegare: si trova lì semplicemente perché si trova nel corpus, e può non trattarsi necessariamente di un'occorrenza frequente. Nel caso di Graham, per esempio, gli elenchi di parole risultanti sono stati sorprendenti per Graham stesso.

Purtroppo, se AntiChildPorn sta usando una simile tecnica, diventa arduo verificare i loro filtri. Nel caso dello spam, ogni utente ha di solito un corpus sufficientemente grande di messaggi e-mail di spam e non, sul quale costruire i propri filtri. Tuttavia non tutti possiedono un altrettanto vasto corpus di materiale pornografico, razzista e simili. A meno che AntiChildPorn non metta a disposizione il suo corpus affinché venga esaminato (cosa piuttosto improbabile), sarà molto difficile valutare le loro tecniche senza mettere insieme un vasto corpus di materiale proibito e vedere come reagisce il loro software.

Se AntiChildPorn sta facendo quel che dice di fare, allora si potrebbe ipotizzare che, talvolta, certi scritti antisemiti possano includere nomi di rabbini. Se AntiChildPorn non sta facendo ciò che dichiara di fare, allora forse hanno buttato nel calderone anche cose come phrack e similari. Senza prove più concrete non è possibile essere più precisi.

Da: "Don Coppersmith" <dcopper@us.ibm.com>

Oggetto: XLS contro Rijndael

Il suo più recente numero di Crypto-Gram induce i lettori a credere che XLS, il lavoro di Courtois e Pieprzyk, abbia violato Rijndael.

Io ritengo che il lavoro di Courtois e Pieprzyk sia errato. Essi sovrastimano il numero di equazioni linearmente indipendenti. Il risultato è che non possiedono sufficienti equazioni lineari per risolvere il sistema, e il metodo non va ad intaccare Rijndael.

Nel dettaglio: Il problema è evidente nel "metodo T'" della sezione 6.3 della loro ristampa di IACR N.2002/044. Loro generano $T' = t' t^{P-1} * \{ \{S-1\} \text{ choose } \{P-1\} \}$ termini che possono essere moltiplicati per x_1 ed ancora rimangono nella loro serie di T monomi, e poi sembrano dichiarare di avere altre nuove equazioni. Ma in realtà, una qualsiasi delle equazioni $t' [t^{P-1} - (t-r)^{P-1}] * \{ \{S-1\} \text{ choose } \{P-1\} \}$ che proviene dalla moltiplicazione di

