

Comunicato stampa in merito ai fondi:
<<http://www.counterpane.com/pr-seriesd.html>>

Comunicato stampa in merito al quarto trimestre:
<<http://www.counterpane.com/pr-2002q4.html>>

*** **

Note di sicurezza da ogni dove: i ciclidi

I ciclidi Midas ricevono la cura di entrambi i genitori: sia il padre sia la madre si occupano degli avannotti. Purtroppo, però, una grande quantità di essi viene uccisa dai predatori. Per evitare di perdere troppi piccoli, i genitori rapiscono i piccoli di altri ciclidi Midas, o anche di altre specie di pesci. (Una volta è capitato che, durante una lotta fra due coppie di ciclidi Midas, il maschio di una terza coppia ne abbia approfittato per riprendersi una cinquantina di avannotti). Ai predatori va benissimo mangiare i piccoli adottati insieme agli altri figli naturali, per cui, finché il branco di piccoli maggiorato non attira altri predatori, il maggior numero di figli naturali sopravviverà.

Il ciclide catturato pratica a sua volta l'adozione, ma è più schizzinoso: adotterà soltanto avannotti più piccoli dei suoi figli naturali. I predatori tenderanno ad attaccare i figli adottivi perché sono più semplici da catturare.

[liberamente tratto da George W. Barlow, "The Cichlid Fishes: Nature's Grand Experiment in Evolution", p. 202-203]

*** **

Il metodo di autenticazione RMAC

Quale parte del processo AES, il NIST ha intrapreso un programma per standardizzare vari metodi operativi per i cifratori a blocchi. A parte i metodi crittografici che già conosciamo dai tempi di DES, NIST sta ora cercando di imporre standard anche sui metodi di autenticazione.

Il primo metodo proposto dal NIST è RMAC (Randomized Message Authentication Code). Esso ha il vantaggio di avere una verifica di sicurezza. Infatti, se si usa triple-DES come cifratore sottostante in una costruzione RMAC (il codice RMAC può funzionare con qualsiasi cifratore a blocchi), la costruzione risultante è dimostrabilmente sicura. Ma questa è esattamente la stessa costruzione che Lars Knudsen ha decodificato in un recente studio.

Che sta succedendo? Da una parte, RMAC è un metodo dimostrabilmente sicuro. Dall'altra esiste un attacco funzionante contro di esso. Non dovrebbe accadere una cosa simile.

Andiamo con ordine...

RMAC è sicuro in qualcosa denominato "modello di cifratore ideale". In quanto parte delle presupposizioni di quel modello, il cifratore a blocchi sottostante necessita di essere sicuro contro svariati attacchi, compresi quelli related-key. Se un cifratore a blocchi è suscettibile ad attacchi di tipo related-key, allora non sarebbe appropriato presentarlo come cifratore ideale, e la verifica di sicurezza di RMAC non si applicherebbe.

Ora, se triple-DES può essere modellato secondo un'algoritmo ideale, allora triple-DES-RMAC dovrebbe risultare sicuro. Infatti, lo standard NIST per RMAC che include triple-DES-RMAC è

una delle due alternative (l'altra è AES-RMAC). Tuttavia, è stato dimostrato come triple-DES non sia sicuro contro attacchi related-key. Ancora peggio, è proprio questa proprietà dell'attacco related-key che Knudsen adopera per decodificare triple-DES-RMAC. Il suo attacco comprende 2^{16} messaggi scelti e circa 2^{56} operazioni, che lo rende alla portata delle risorse informatiche odierne.

Così ora possiamo spiegare che cos'è accaduto. La verifica di sicurezza per RMAC funziona soltanto se si assume l'utilizzo di un cifratore ideale. Se è necessario trarre delle conclusioni su RMAC con un vero cifratore a blocchi come triple-DES o AES, bisogna sperare che quel cifratore a blocchi reale si comporti come un cifratore ideale a sufficienza affinché la stessa verifica continui a resistere. Nel caso di triple-DES quella speranza si è vanificata. Triple-DES non è modellato abbastanza bene per essere un algoritmo ideale, dato che è vulnerabile agli attacchi di tipo related-key. Come ha dimostrato Knudsen, se sussistono attacchi di tipo related-key sul proprio cifratore a blocchi reale, questo non solo rende la verifica irrilevante e "invalida" la garanzia di sicurezza, ma può anche portare gravi attacchi all'RMAC.

A questo punto, il quesito più interessante è chiedersi se AES-RMAC è sicuro. Se si vuol pensare che la verifica di sicurezza per RMAC dica qualcosa in merito ad AES-RMAC, occorre sperare che AES si comporti come un cifratore ideale. Una condizione necessaria è che AES debba essere sicuro contro attacchi di tipo related-key.

AES è un nuovo cifratore, e la sua sicurezza contro gli attacchi related-key non è stata ancora approfonditamente studiata. La maggior parte dei crittoanalisti si concentra sul modello di minaccia standard (attacchi di tipo testo in chiaro/cifrato scelto), e gli attacchi related-key sono solo occasionalmente studiati. Quel poco che sappiamo in merito alla sicurezza di AES contro attacchi related-key suggerisce che AES è considerevolmente più debole contro questi attacchi rispetto ad attacchi normali: il migliore attacco related-key (scoperto dopo soltanto alcune settimane di analisi) rompe nove round.

La morale qui è che il modello di cifratore ideale non è uno strumento così potente come molti tendono a pensare, ed un metodo operativo che è sicuro in quel modello non è necessariamente sicuro nella pratica. La teoria crittografica è abbastanza matura per basarvi dei progetti, ma non esiste ancora un sostituto della crittoanalisi dettagliata. RMAC non dovrebbe diventare uno standard NIST.

Le specifiche NIST per RMAC:

<<http://csrc.nist.gov/publications/drafts/draft800-38B-110402.pdf>>

La pagina dei metodi operativi del NIST:

<<http://csrc.nist.gov/encryption/modes>>

Commenti su RMAC:

<<http://csrc.nist.gov/encryption/modes/comments/>>

Le analisi di David Wagner, Phil Rogaway, e di Lars Knudsen sono particolarmente degne di nota.

Gli attacchi related-key contro triple-DES:

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

Gli attacchi related-key contro AES:

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

Questo articolo è stato scritto con l'aiuto di David Wagner.

Non esiste una struttura a cui riferirsi quando si tratta di proteggere la nostra proprietà e le nostre macchine da continui attacchi. Ce n'è bisogno. L'altra grande differenza è che il progetto di legge Berman propone che sia permesso al detentore del copyright di prendere provvedimenti contro persone *che stanno commettendo un crimine*. La presunta attività è contro la legge -- ma se si configura in rete una macchina Windows 2000 e questa viene infettata da Nimda e si mette ad attaccare chiunque ininterrottamente, questo *non* è un crimine. Non vi è nulla di illegale nell'essere stupidi o al non sapere come rendere sicuro un sistema.

Dobbiamo guardare tutto questo entro i confini del blocco di un processo di attacco -- non possiamo farne una questione "personale" come se stessimo facendo qualcosa contro le persone che possiedono queste macchine. In effetti la legge corrobora questa differenziazione: se io configuro una macchina Windows 2000 con i parametri di default, sapendo che verrà compromessa nel giro di 10 minuti ed inizierà ad attaccare altre macchine "vicine", io non ho commesso un crimine. Però, se io attivo uno script Perl che esegue le stesse identiche richieste GET contro le stesse identiche macchine, io ho commesso reato.

Se il legame fra un amministratore e le azioni commesse dalle sue macchine non può sostenere la colpevolezza per azioni in caso di danno (ovvero l'essere ritenuti responsabili perché i loro computer sono stati infettati da Nimda), come possiamo sostenere la stessa logica necessaria ad affermare che stiamo violando i diritti dell'amministratore quando neutralizziamo l'attacco? Perché pretendiamo di sostenere che la macchina abbia dei diritti?

Anche se sostenessimo che la macchina abbia qualche diritto sottinteso, dovremmo trattarla come si fa con un criminale: se le azioni di un individuo mostrano che egli non può agire nella società civile senza nuocere agli altri o calpestare i diritti altrui, gli vengono tolti i suoi diritti e gli viene impedito di agire di conseguenza. La mera infezione di un sistema a causa di un worm mostra che questo sistema non è configurato in modo appropriato per convivere in un network globale -- perciò esso perderà alcuni "diritti" (che non penso dovrebbe avere, in primo luogo).

Analogie con il comportamento da padrone di casa non funzionano mai realmente: ci sono semplicemente troppe cose che uno può dire in un modo o nell'altro per ottenere il risultato desiderato. Devo invadere la proprietà di un vicino per fermare la fonte di disturbo? Probabilmente no, ma qualcuno potrebbe farlo, secondo una certa ottica della legge sulla turbativa. Potrei sempre replicare che se la mia motocicletta è stata rubata, e io l'ho poi vista nel tuo giardino, io ho tutto il diritto di entrare nella tua proprietà per riprendermela -- la legge dice che posso. E allora dove ci si ferma?

Se lei intendeva rendere l'analogia più appropriata alla questione, occorrerebbe dire che l'allarme di casa non solo faceva rumore di suo, ma che ha causato l'attivazione degli allarmi adiacenti, i quali hanno causato l'attivazione degli allarmi ad essi adiacenti, eccetera eccetera. Molto presto tutti devono urlare per farsi sentire. Nessun rumore di questo genere è contro la legge, per cui la polizia non potrà intervenire. Il produttore degli allarmi sostiene che non è un problema suo, ma è colpa del padrone di casa se non sa come installarli. In più, tutti i criminali sanno che le case con gli allarmi scattati sono assolutamente aperte, e così essi usano l'allarme come segnale per rintracciare abitazioni da sfruttare per qualche futura attività illecita. Ciò che è davvero triste capita quando si cerca di parlare con i vicini in merito al rumore e questi rispondono "Quale rumore? Non sentiamo nessun rumore. Se ne vada".

Da: John Kelsey <kelsey.j@ix.netcom.com>
Oggetto: Il contrattacco

Solo un piccolo appunto riguardo al suo articolo sul contrattacco: non credo che la giustizia possa contare sul governo per l'assegnazione di una pena (si pensi a un governo davvero corrotto, dove la pena viene sempre assegnata a chi ha pagato la tangente più bassa). Fare in modo che sia una terza parte neutrale ad indagare i fatti e a decidere quale pena o

risarcimento si debba applicare, è un modo per fare giustizia in merito di pene e risarcimenti, ma non è né l'unico sistema per ottenerla, né si ha la garanzia di ottenerla. E quella terza parte neutrale può essere o non essere il governo.

Un esempio veramente ovvio di giustizia fatta da un'entità "non governativa" è quando un genitore stabilisce con esattezza quale dei figli ha incominciato la rissa e assegna una punizione in maniera adeguata.

È altrettanto ovvio constatare come i contrattacchi automatizzati siano una pessima idea in quasi tutti i casi. Non solo è arduo garantire che il proprio sistema automatizzato identifichi esattamente l'assalitore, ma è altresì arduo garantire che il proprietario del sistema che contrattacca non abbia generato lui stesso la prova dell'attacco iniziale per giustificare il suo contrattacco. Ed è facile immaginare una "guerra" fra due o tre sistemi del genere. (Si noti come questi siano tutti problemi che compaiono anche nei casi di vigilantismo: la folla che impicca la persona sbagliata, la folla viene aizzata dalle false accuse dei nemici del capro espiatorio, oppure voi mi linciate, e poi i miei amici e la mia famiglia linciano voi).

Da: Paul Mantyla <pjm1212@yahoo.com>

Oggetto: Il contrattacco

Nel numero di Crypto-Gram del 15 dicembre, lei sostiene che "le leggi ci danno il diritto di giustizia..." Questa è un'affermazione troppo forte, e quel che dice dopo non corregge l'errore. Solo un essere onnisciente è in grado di stabilire che cosa è giusto.

Una serie di leggi e di diritti civili sono la nostra migliore approssimazione a questo proposito. Come notoriamente disse Oliver Wendell Holmes "Questo è un tribunale di leggi, giovanotto, non di giustizia". È giusto che un uomo colpevole sia a piede libero, o che un innocente sia imprigionato? Il governo diventa molto pericoloso quando ignora la legge e la Costituzione per seguire la giustizia. Per esempio, in apparente violazione della protezione del Quinto Emendamento (che vieta di processare qualcuno per un reato per il quale è già stato assolto la prima volta), la dottrina nota con il nome "duplice sovranità" permette ai governi statale e federale di perseguire un individuo per lo stesso reato (per esempio gli ufficiali di polizia nel caso Rodney King).

Si veda "An Ever-Expanding Double Jeopardy Loophole" nel Cato Institute's Handbook for Congress: <<http://www.cato.org/pubs/handbook/hb105-22.html>>. Quali cittadini degli Stati Uniti, abbiamo diritto a molte cose, ma un "diritto alla giustizia" non è fra queste.

Da: Daniel Upper <upper@peak.org>

Oggetto: Il contrattacco

Finché i tribunali non stabiliranno in quali casi è permesso il contrattacco, vorrei suggerire la difesa della necessità quale spunto di riflessione a riguardo. In genere, chi si difende non è colpevole di aver violato una legge se era necessario difendersi. I criteri per stabilire questa necessità possono variare, ma in via generale potrebbero essere così riassunti:

- * L'azione è stata compiuta per allontanare la minaccia di un danno immediato e significativo.
- * Il danno causato dall'azione non è stato sproporzionato al danno evitato.
- * Non esiste un'alternativa legale ragionevole all'azione.
- * Chi ha agito credeva ragionevolmente che la sua azione avrebbe prevenuto il danno significativo.

* Chi si è difeso non è stato causa della minaccia di tale danno.

Questa verifica è abbastanza rigorosa è applicabile su vasta scala. La maggior parte delle eccezioni d'emergenza (difesa personale, pronto soccorso effettuato da personale non medico) possono essere viste come casi particolari. Mi aspetto che qualsiasi tipo di contrattacco che la legge soddisferà anche questi criteri.

Si noti inoltre come qui giustizia e pena non vengano affatto nominate: si sanziona unicamente la prevenzione di un danno.

Da: Michael Nygard <mtnygard@charter.net>

Oggetto: Il contrattacco

C'è una sfumatura alle varie proposte in materia di contrattacco che mi spiace non aver visto analizzata nel suo intervento. La differenza fondamentale sta fra una vendetta e una difesa personale. Se si è vittime di un crimine, si ha il diritto di difendersi -- mentre il crimine viene commesso.

Così come l'irruzione in una abitazione può degenerare da furto a omicidio in pochi caotici istanti, dobbiamo riconoscere come un'intrusione possa degenerare da minima a catastrofica nel giro di millisecondi. Malgrado questo sia ancora un punto di controversia fra chi emana le leggi e chi le fa rispettare, la difesa personale è ampiamente riconosciuta come metodo per evitare che una situazione degeneri. I contrattacchi automatizzati hanno la medesima funzione: limitare i danni commessi dall'assalitore, magari evitando che il reato degeneri da semplice vandalismo a furto di enormi proporzioni.

Sarebbe semplicistico affermare che lo stesso atto sia difesa personale nel momento in cui viene commesso un reato, ma vigilantismo dopo. Tuttavia, quando le forze dell'ordine non possono rispondere durante il crimine stesso, un rapido contrattacco potrebbe rivelarsi l'unica forma di protezione disponibile.

Da: Brian Beesley <BJ.Beasley@ulster.ac.uk>

Oggetto: Il contrattacco

Vi sono due punti che forse le sono sfuggiti:

(1) Se è ammesso che X possa contrattaccarti sulla base che X sospetta (forse possiede persino prove inconfutabili) che tu stia attaccando X in qualche modo, allora perché non è possibile che tu possa contro-contrattaccare? Ciò che voglio dire è che se in questo caso X è il "pezzo grosso" e vi sono molte persone nella mia posizione, noi (agendo di comune accordo) abbiamo più probabilità di infliggere seri danni a X che il contrario.

(2) Il meccanismo del contrattacco è legato al nostro lasciare i computer esposti ad attacchi e/o seguendo una condotta imprudente (ad esempio lanciando script scaricati da pagine Web). Questa strategia potrebbe essere abbastanza fruttuosa contro utenti casuali, ma non avrà molto effetto su qualcuno che decida di sua volontà di agire "illegalmente".

La "legge Berman" fa inevitabilmente acqua da tutte le parti -- non a causa del suo contenuto politico, ma perché sbaglia l'approccio al problema. La legislazione proposta è designata per "suonare bene" ai suoi proponenti, più che essere di qualche efficacia.

Semplicemente, non c'è bisogno di ulteriore legislazione, a nessun livello, nella maggior parte del mondo civilizzato. Ciò che serve è la volontà da parte di chi si sente derubato della sua

proprietà intellettuale di raccogliere prove che potrebbero essere presentate nell'ambito dell'attuale legislazione, invece di lamentarsi delle proprie (dubbie) perdite di profitti.

Da: Mike Koptiw <mkoptiw@att.net>

Oggetto: Il contrattacco

Sono d'accordo sul fatto che il vigilantismo sia moralmente sbagliato, e sono d'accordo sul fatto che lo stato è il più adatto ad occuparsi della giustizia. Però, nel contesto di una diatriba legale, traccerei una distinzione fra una reazione ad un attacco DOS e una reazione ad una violazione di copyright.

Come sempre, dipende dalle circostanze. In alcuni casi, i principi generali del diritto comune in merito al torto privilegiano l'azione della vittima contro l'assalitore. Anzitutto, il diritto comune non incoraggia l'uso della forza per riprendersi una proprietà persa. I tribunali risolvono tali questioni. La legge si occupa di questo, e non si tratta di vigilantismo.

Tuttavia, il diritto comune incoraggia l'uso della forza in difesa di una proprietà contro trasgressori violenti. La forza che è concesso usare deve essere proporzionata all'espulsione del trasgressore, e una volta che il trasgressore abbia lasciato la proprietà, non è concesso alla vittima di continuare l'uso di tale forza ai danni del trasgressore.

Perciò ritengo che possano sussistere teoriche diatribe legali basate sul diritto comune per quanto concerne le reazioni in caso di attacchi DOS e hacking intrusivo, in cui esiste un trasgressore virtuale (che sia un pacchetto DOS pericoloso o la presenza di un hacker), ma non vi è alcun sostegno legale a cui aggrapparsi quando l'attacco è basato unicamente sul recupero di un diritto sui contenuti del computer di qualcuno (come vorrebbe la proposta della RIAA).

Da: Marko Asplund <aspa@kronodoc.fi>

Oggetto: Il contrattacco

Oltre ad essere un'idea discutibile eticamente e moralmente, non riesco a capire come la tecnologia di contrattacco automatizzato potrebbe salvare Internet dagli attacchi worm totali. Il contrattacco potrebbe forse avere buon esito contro worm attuali come Nimda, che decidono di lasciare la porta aperta quando entrano, ma è ingenuo pensare che worm di una prossima generazione continueranno a farlo.

Stabilire le varie responsabilità è assai arduo nel caso il contrattacco fallisca. Anche se esso si serve della minima forza e massima cura viene impiegata nel preparare il codice neutralizzante, è sempre possibile che qualcosa vada storto e il sistema bersaglio fallisca in qualche modo dopo la neutralizzazione. Che cosa accadrebbe se il sistema infettato controllasse in un ospedale gli impianti che permettono la sopravvivenza? Se vengono perdute delle vite umane a causa del contrattacco, chi è responsabile se i sistemi smettono di funzionare dopo il contrattacco? Vi è sempre un ridotto numero di patch prodotte dai produttori di software che hanno esiti imprevisti su alcuni sistemi. Perché non potrebbe accadere lo stesso con questi sistemi di contrattacco?

Mullen traccia un parallelo fra la difesa personale e il contrattacco, ma una differenza è che un sistema software in Internet non possiede la stessa intelligenza o quantità di informazioni sul contesto dell'attacco o sull'assalitore rispetto ad un essere umano sotto attacco. Sfruttando la sua analogia del vicino rumoroso, uno potrebbe dire che il contrattacco è come cercare di disattivare il dispositivo rumoroso con una pistola...ma sparando alla cieca.

Da: Rick Bressler <bressler@the-bresslers.com>
Oggetto: Il contrattacco

Dopo aver letto il suo intervento e aver riflettuto un po', mi chiedo se non ci troviamo di fronte all'inizio di una dottrina di "autodifesa" su Internet, anche se a questo punto molta della legislazione è chiaramente fuori luogo e inadeguata, come accade spesso quando chi emana le leggi cerca di adattarsi a nuovi scenari.

Penso si possa dire che i suoi confronti con il crimine nel mondo reale tralascino completamente il concetto di difesa personale (o questo è intenzionale?). Nel mondo reale c'è una grossa differenza tra difesa personale, attacco preventivo e vigilantismo. Vi è un'estesa casistica giudiziaria in merito a tutti e tre.

Ovviamente un attacco preventivo è illegale (a meno di essere un governo, naturalmente :-)). Non è ammesso attaccare qualcuno solo perché si ritiene che questi *possa* attaccare in futuro.

Il vigilantismo è attaccare l'aggressore dopo il fatto, o cercare di farsi giustizia da soli. Chiaramente questo non può essere permesso in una società civile, né viene tollerato da alcun sistema legale di mia conoscenza, anche se in diversi tempi e luoghi è stato giustificato.

La difesa personale è una risposta alla minaccia immediata, che sia di morte o di grave danno fisico. Ha un posto questa dottrina, nel mondo virtuale? Nel suo esempio di qualcuno che attacca intenzionalmente una macchina o, meglio, un server di una importantissima infrastruttura, e della vittima che risponde all'attacco disattivando l'aggressore, abbiamo una situazione analoga, in certa misura, alla difesa personale nel mondo reale; almeno nella misura in cui uno stia reagendo ad una minaccia immediata e probabilmente grave; magari una minaccia che potrebbe essere temporaneamente "letale" per Internet.

Si noti come nel mondo non-virtuale ci riserviamo questo diritto solo per i crimini più efferati, come la minaccia nei confronti di vite innocenti e, in rari casi, di proprietà "innocenti". Esiste un caso in cui questo possa essere esteso ad un "server innocente"? Forse quello che protegge la propria rete domestica? O la propria carta di credito? O il conto in banca? O un esiguo numero di server da cui tutta Internet dipende?

Da: Nicholas Weaver <nweaver@CS.berkeley.edu>
Oggetto: Un caso in cui il vigilantismo ha funzionato...

Esiste un caso in cui il vigilantismo ha funzionato: lo script `das-bistro anti-code-red-II default.ida`.

Questo script, una volta installato su un web server, rispondeva ad un attività di probing di Code Red II con un contrattacco che disabilitava il web server che faceva uso della backdoor di Code Red II e poi riavviava la macchina, ripulendola dall'infezione di Code Red II (residente in memoria) e prevenendo successive infezioni e abusi della macchina.

Considerando che tutte quelle macchine stavano comunicando a tutto il mondo di essere banalmente vulnerabili, eliminarle dalla rete è probabilmente indispensabile, soprattutto perché non c'è nessuna polizia da chiamare: non esiste un metodo standard per affermare che "questa macchina è compromessa" e fare in modo che il provider Internet prenda provvedimenti a riguardo.

Qualche malintenzionato avrebbe potuto facilmente modificare e rilasciare CRclean (un codice sorgente "antiworm" passivo pubblicato su BugTraq) con un contenuto malintenzionato per selezionare tutte quelle macchine. Per cui, avere un certo numero di pagine web contro Code Red II è stato probabilmente un vantaggio.

Naturalmente ciò ha funzionato grazie alla stupidità e/o ingenuità strategica degli autori di Code Red II (mai creare canali di controllo che possano essere usati da chiunque senza autorizzazione e chiudere sempre il passaggio da cui si è entrati).

Da: "John.Deters" <John.Deters@target.com>
Oggetto: Il contrattacco

Nel suo articolo, lei sostiene che il vigilantismo sia sbagliato, che sia un'idea che è stata "sempre evitata dalle società civili".

Lei non sembra considerare che Internet è un nuovo *genere* di società civile. Per la prima volta nella storia, abbiamo una società che non è vincolata alla geografia. Tutti i sistemi giudiziari erano e sono ancora vincolati a confini geopolitici. Ma i pacchetti IP non fanno richiesta di visti prima di oltrepassare quei confini. I cavi e le fibre portano merci, servizi, e illegalità nella stessa maniera e senza pregiudizi. Quindi avviene il commercio, regolamentato e tassato solo da quelle persone abbastanza ingenui che richiedono spontaneamente ai loro governi di essere regolamentati e tassati per le loro attività on-line. Anche l'illecito ha luogo, ma i malintenzionati solitamente non sentono il bisogno di render conto delle loro attività.

Inoltre, la definizione di illecito varia a seconda della propria prospettiva. La RIAA ritiene che l'illecito abbia luogo quando si scarica un brano. Io ritengo che accada quando ricevo dello spam o qualche stupido virus via e-mail. Lei ritiene che accada quando i suoi clienti ricevono attacchi DDOS.

Non esiste un governo globale che regola questa società che è Internet. Tutto ciò che abbiamo è un insieme variegato di agenzie, vincolate geograficamente, che fanno rispettare le leggi e si mettono a caccia dei malintenzionati. A volte si fermano entro i propri confini, altre volte chiamano rinforzi dall'altra parte in modo che eseguano l'arresto in loro vece. Nella maggior parte dei casi non fanno nulla.

Per cui, in una società essenzialmente senza leggi, una società che non ha ancora formato un governo coesivo, solido, una società che permette a un malintenzionato di nascondersi fra un governo e l'altro, che cosa ci si aspetta dalle persone quando nessuno è in grado di fare giustizia? Non dovrebbero fare nulla? Dovrebbero chiamare l'FBI? Dovrebbero richiedere un Governo Globale di Internet?

I vigilanti non stanno semplicemente "facendosi giustizia da soli", perché solitamente non c'è una legge che possa venire applicata. Per cui se un hacker perseguita il computer di uno spammer, me ne rallegro. Se la RIAA perseguita il computer di un utente di Napster, non me ne importa affatto. In Internet mi difendo da solo, e tante grazie. Ma una cosa che sono assolutamente sicuro di non voler vedere è un'agenzia di regolamentazione globale che decida o meno di "approvare" i pacchetti che spedisco. Perché non ho dubbi che qualsiasi cosa io invii o riceva, sia essa musica, immagini, o un'e-mail sovversiva a qualche newsletter sulla crittografia, una ristretta cerchia di persone si sentirà lesa e richiederà il mio arresto.

Da: "Tousley, Scott W." <Scott.Tousley@anser.org>
Oggetto: Il Dipartimento per la Sicurezza Nazionale

Nel numero di Crypto-Gram di dicembre, fra i suoi commenti a riguardo del Dipartimento per la Sicurezza Nazionale, lei ha scritto: "La sicurezza ha due evidenti verità, assai utili per questa discussione:

1) Le decisioni riguardanti la sicurezza devono essere prese il più vicino possibile al problema. [...] 2) L'analisi sulla sicurezza deve avvenire il più lontano possibile dalle fonti."

Non sono completamente d'accordo sul punto 2), perché l'analisi sulla sicurezza di eventi rari deve essere sia centralizzata che decentralizzata. L'analisi sulla sicurezza è sempre più una sfida distribuita che continuerà ad implicare una miscela assennata di sistemi e persone, e questa sfida di analisi richiede un certo contesto che può venire soltanto dalla vicinanza. Occorre permettere in qualche modo un'analisi efficiente da parte di analisti nazionali e internazionali, che parta dal livello più basso della guardia giurata, fino al più alto, del supervisore in prima linea. Poliziotti, guardie e personale di pronto intervento possono combattere il terrorismo in modo efficiente soltanto se essi stessi sono minimamente coinvolti e contribuiscono al più ampio contesto d'analisi. La forza, flessibilità ed evoluzione delle reti possono sostenere gran parte di questo bisogno, a meno che queste reti ancora neonate non vengano schiacciate dagli interessi burocratici di un Dipartimento per la Sicurezza Nazionale e da varie controparti statali e municipali mentre si azzuffano per un posto alla mangiatoia. Mi preoccupa il fatto che la nostra riorganizzazione renderà la sicurezza ancora più fragile mentre siamo impegnati a fare grandi manovre di coordinamento nel nome dell'efficienza politica, burocratica e di bilancio.

Da: The Wengers <wenger@bigfoot.com>

Oggetto: Il Dipartimento per la Sicurezza Nazionale

Concordo con il suo punto di vista quando afferma che un'intelligence dedicata all'analisi non debba affidarsi unicamente al nuovo Dipartimento per la Sicurezza Nazionale. Ma noto da alcuni segnali molto fastidiosi che l'ago della bilancia sia stato spostato un po' troppo dall'altra parte, così da poter proteggere il territorio delle agenzie preesistenti.

La tensione sta nel creare una serie di giurisdizioni sovrapposte in modo che le cose non finiscano fra le fessure, ma non troppo sovrapposte per non creare inutili ridondanze e lotte per il territorio. Perciò mi ha infastidito leggere un recente articolo sul Washington Post intitolato "Homeland Security Won't Have Diet of Raw Intelligence Rules Being Drafted to Preclude Interagency Conflict" (di Dan Eggen e John Mintz, 6 dic. 2002, pag. A43) [lett. "La Sicurezza Nazionale non avrà una dieta di regole di intelligence pura, per evitare conflitti fra agenzie"]. L'articolo fa notare che "per ora, le agenzie di intelligence hanno convinto la Casa Bianca che le informazioni fornite al Dipartimento per la Sicurezza Nazionale dovrebbero essere redatte in forma di rapporti riassuntivi. Questi riassunti non comprenderanno informazioni di prima mano né dettagli su dove e come tali informazioni sono state raccolte, in modo da proteggere le fonti e i metodi".

Potrebbe non avere senso sollevare le agenzie di intelligence già esistenti dai loro ruoli di raccolta ed analisi di informazioni, per i motivi che lei ha già illustrato. Tuttavia, se a questo Dipartimento per la Sicurezza Nazionale bisogna assegnare un qualche ruolo importante, esso dovrebbe riguardare il coordinamento dell'analisi di minaccia e di risposta. Non credo che questo lavoro possa venire svolto in maniera efficiente se ci si deve affidare a dati di seconda mano. Come lei ha giustamente affermato "È importante che tutte queste organizzazioni comunichino fra loro, ed è questo il valore primario di un Dipartimento di Sicurezza Nazionale. Un'organizzazione dovrà essere l'unico centro di coordinamento ed analisi delle minacce e delle risposte terroristiche. Un'altra avrà il compito di occuparsi del 'disegno generale', prendere decisioni e impostare regole di condotta in base ad esso". Ma come può il Direttore del Dipartimento per la Sicurezza Nazionale vedere questo "disegno generale" e prendere decisioni pienamente informate se il suo team non può visionare i dati sui quali sono basate le

conclusioni che deve trarre? Questi sforzi, da parte di CIA, NSA ed FBI, di tenere il muso della Sicurezza Nazionale fuori dalla mangiatoia delle informazioni di intelligence, non possono essere un buon segno.

L'articolo del Washington Post continua facendo notare che "i funzionari dell'Amministrazione, per esempio, stanno già valutando se includere o meno i rappresentanti della sicurezza nazionale fra i membri delle 56 Task Force Antiterrorismo regionali, che sovrintendono alle indagini di terrorismo locale". Come può essere questo un motivo di discussione? Se si legge la descrizione dell'FBI del programma di queste Task Force, essa comprende rappresentanti di una gran quantità di agenzie federali insieme ad agenzie statali e persino locali. "Vi sono al momento 36 Task Force operative, il che significa un aumento di 25 task force dal 1996, alle quali sono assegnati più di 620 agenti speciali dell'FBI, e circa 584 ufficiali part-time e a tempo pieno provenienti da altre agenzie federali, statali e locali. I partecipanti federali a tempo pieno nel programma Task Force Antiterrorismo comprendono: Immigration and Naturalization Service; U.S. Secret Service; Naval Criminal Investigative Service; U.S. Marshals Service; U.S. Customs Service; Bureau of Alcohol, Tobacco, and Firearms; U.S. Border Patrol; U.S. Department of State/Diplomatic Security Service; Postal Inspection Service; Internal Revenue Service; Department of Interior's Bureau of Land Management; Air Force Office of Special Investigations; U.S. Park Police; Federal Protective Service; Treasury Inspector General for Tax Administration; e il Defense Criminal Investigative Service." (13 nov. 2001, Dichiarazione per la documentazione di Kathleen McChesney, vicedirettore della Training Division, FBI, in comunicazione con la Law Enforcement Community di fronte allo United States House of Representatives Committee in merito alle riforme governative. Washington, D.C. <<http://www.fbi.gov/congress/congress01/mcchesney111301.htm>>)

Diciamolo chiaramente, la Park Police e il Bureau of Land Management sono rappresentati nelle Task Force Antiterrorismo, ma NON il Dipartimento per la Sicurezza Nazionale? Come può essere un buon segno, questo?

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

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.

Copyright (c) 2003 by Counterpane Internet Security, Inc.