



Il principio di Kerckhoffs non menziona l'effettiva pubblicazione di algoritmi e protocolli, ma soltanto il requisito per rendere la sicurezza indipendente dalla loro segretezza. Ai tempi di Kerckhoffs non esisteva una vasta comunità crittografica che potesse analizzare e criticare i sistemi crittografici, per cui non si traeva un gran beneficio dalla pubblicazione. Oggi invece vi è un enorme beneficio derivante dalla pubblicazione, e si ottiene un beneficio ancora maggiore dall'utilizzo di modelli già pubblicati ed analizzati da altri. Mantenere segreti questi modelli non è altro che inutile oscurità. Il principio di Kerckhoffs sostiene che non deve esistere alcun impedimento legato alla sicurezza che sbarrì la strada alla pubblicazione; l'attuale comunità crittografica dimostra continuamente che si trae enorme vantaggio dalla pubblicazione.

Il beneficio è la cosiddetta peer review, cioè la revisione tra esperti di pari livello. La crittografia è difficile, e quasi tutti i sistemi crittografici non sono sicuri. Ci vuole l'intera comunità crittografica, e anni di lavoro, per esaminare accuratamente un sistema. La quasi totalità dei sistemi crittografici sicuri sono stati sviluppati con algoritmi e protocolli pubblicati e di pubblico dominio. Non mi sovviene alcun sistema crittografico sviluppato in segreto che - una volta reso pubblicamente noto - non abbia avuto difetti scoperti dalla comunità crittografica. Questo comprende l'algoritmo Skipjack e il protocollo Clipper, entrambi sviluppati dalla NSA.

A corollario del principio di Kerckhoffs si può dire che meno segreti possiede un sistema, più esso si rivela sicuro. Se la perdita di un segreto qualsiasi provoca il fallimento del sistema, allora il sistema con il minor numero di segreti è il più sicuro. Più segreti un sistema possiede, più è fragile. Un minor numero di segreti indica maggiore robustezza.

Questa regola, generalizzata, può applicarsi ad altri generi di sistemi, ma non è sempre facile capire in che modo. Meno segreti vi sono, più sicuro si rivela essere un sistema. Sfortunatamente, discernere quali segreti siano richiesti non è sempre ovvio. Ha senso che le compagnie aeree pubblichino i criteri di ricerca del personale da imbarcare? Ha senso che l'esercito pubblichi le proprie metodologie riguardanti la disposizione delle mine su un territorio? Ha senso che un'azienda pubblichi la topologia completa del proprio network, o dei propri sistemi di sicurezza, o le impostazioni dei propri firewall? Quando la segretezza è necessaria per la sicurezza, e quando risulta essere solo oscurità?

Esiste una sequenza di requisiti di segretezza, e sistemi differenti vengono a trovarsi in punti differenti lungo questa sequenza. La crittografia, grazie alla propria natura matematica, permette al progettista di riunire tutti i segreti richiesti per la sicurezza in un'unica chiave (o anche in chiavi multiple, talvolta). Altri sistemi, invece, non sono così netti. La sicurezza aerea, ad esempio, incorpora dozzine di potenziali segreti: come uscire sulla pista di atterraggio, come penetrare nella cabina di pilotaggio, il disegno dello sportello della cabina di pilotaggio, le procedure di monitoraggio di passeggeri e bagagli, le impostazioni esatte del sistema di rilevamento di esplosivi, il software del pilota automatico, ecc. La sicurezza dell'intero sistema aereo può essere minata se viene scoperto uno di questi segreti.

Ciò significa che la sicurezza aerea è fragile. Un gruppo di persone è a conoscenza di come è stato progettato il rinforzo per lo sportello della cabina di pilotaggio. Un altro gruppo ha programmato vari criteri di monitoraggio all'interno del software per le prenotazioni. Altri gruppi hanno progettato l'equipaggiamento per esaminare i passeggeri. Un altro gruppo ancora è a conoscenza di come raggiungere la pista d'atterraggio e danneggiare l'aereo. Il sistema può essere attaccato tramite uno qualsiasi di questi modi. Ma non esiste una maniera semplice per applicare il principio di Kerckhoffs alla sicurezza aerea: vi sono troppi elementi da tenere segreti e non c'è modo di riunirli tutti in una singola "chiave". Ciò non significa che sia impossibile rendere sicura una linea aerea, ma soltanto che è più difficile. E che la fragilità è un elemento intrinseco alla sicurezza aerea.

Altri sistemi possono essere analogamente presi in considerazione. Di certo, l'esatta dislocazione di mine in un territorio fa parte della "chiave", e dev'essere mantenuto segreto. L'algoritmo utilizzato per disporre le mine non ha il medesimo livello di segretezza, ma

mantenerlo segreto può giovare alla sicurezza generale del sistema. In un network, la configurazione del firewall e degli ID è tenuta in maggior segreto rispetto alla dislocazione fisica di quei sistemi sul network stesso, che è a sua volta tenuta in maggior segreto rispetto al genere di dispositivi impiegati. Gli amministratori di rete dovranno decidere con precisione che cosa mantenere segreto e che cosa non sia motivo di preoccupazione. Ma più aumenteranno i segreti, più difficoltosa e fragile risulterà la sicurezza.

Il principio di Kerckhoffs è soltanto metà del processo decisionale. Soltanto perché la sicurezza non richiede espressamente che qualcosa sia tenuto segreto, questo non vuol dire che sia automaticamente una buona mossa pubblicizzarlo. Vi sono due caratteristiche che rendono di estrema efficacia la pubblicazione in ambito crittografico. La prima è che esiste un vasto gruppo di persone capaci e intenzionate ad esaminare i sistemi crittografici, e la pubblicazione è un modo per incanalare le loro abilità. La seconda è che esistono altre persone che hanno bisogno di realizzare sistemi crittografici e sono sulla stessa barca, e quindi ognuno può apprendere dagli errori dell'altro. Se la crittografia non avesse queste caratteristiche, non vi sarebbe alcun beneficio nella pubblicazione.

Nel prendere decisioni riguardanti altri sistemi di sicurezza, è importante ricercare queste due caratteristiche. Prendiamo ad esempio un pulsante di emergenza all'interno della cabina di pilotaggio di un aereo. Supponiamo che il sistema sia stato progettato in modo tale per cui la pubblicazione di questo particolare non comprometta la sicurezza generale. Il governo dovrebbe divulgarlo? La risposta dipende dalla presenza o meno di una comunità di professionisti che possa analizzare la progettazione di quel dispositivo di emergenza. Se questa comunità non è presente, allora non ha senso divulgarlo.

L'algoritmo per la guida dei missili è un altro esempio. Sarebbe una mossa sensata da parte del governo pubblicare i propri algoritmi per pilotare i missili? Credo che la risposta non possa essere che negativa, perché il sistema manca della seconda caratteristica vista prima. Non esiste una vasta comunità di persone che possa beneficiare di queste informazioni, ma vi sono potenziali nemici che invece ne potrebbero trarre giovamento. Perciò è preferibile, da parte del governo, mantenere segrete le informazioni e rivelarle solamente a coloro che si ritiene debbano esserne informati.

Dato che la segretezza richiesta per la sicurezza è raramente una questione dai contorni netti, pubblicare ora diventa un elemento di compensazione verso la sicurezza. E, sempre in ambito di sicurezza, il beneficio derivante dalla segretezza è più importante dei benefici conseguenti alla pubblicazione? Potrebbe non essere una decisione facile da prendere, ma si tratta di una decisione precisa.

Storicamente, la NSA non ha mai pubblicato i propri dettagli crittografici - non perché la loro segretezza aumentava la sicurezza, ma perché non intendevano offrire ai loro nemici della "guerra fredda" i benefici della loro perizia.

Si può generalizzare il principio di Kerckhoffs nella seguente linea guida progettuale: si riducano al minimo i segreti nel proprio sistema di sicurezza. Finché si riesce ad ottenere questo obiettivo, si aumenta la robustezza della sicurezza generale del sistema. Quando si arriva a non ottenerlo più, è la fragilità generale ad aumentare. Tenere nascosti certi dettagli del sistema è una decisione ben distinta dal mantenere sicuro il sistema, a prescindere dalla divulgazione; essa dipende dall'esistenza di una comunità che possa analizzare quei dettagli e dall'esistenza di gruppi di "buoni" e "cattivi" che possano sfruttare quei dettagli per rendere sicuri altri sistemi.

Il trattato di Kerckhoffs (in francese):

<[http://www.cl.cam.ac.uk/~fapp2/kerckhoffs/la\\_cryptographie\\_militaire\\_i.htm](http://www.cl.cam.ac.uk/~fapp2/kerckhoffs/la_cryptographie_militaire_i.htm)>

Un altro saggio dello stesso genere:

<<http://online.securityfocus.com/columnists/80>>



[purloined\\_voice\\_mail\\_3](#)>

<<http://www.computerworld.com/securitytopics/security/story/0,10801,70048,00.html>>

Interviste interessanti a Ralph Merkle e a Whitfield Diffie sull'invenzione della crittografia a chiave pubblica:

<<http://www.itas.fzk.de/mahp/weber/merkle.htm>>

<<http://www.itas.fzk.de/mahp/weber/diffie.htm>>

Una vignetta sulla sicurezza delle linee aeree:

<<http://images.ucomics.com/comics/bz/2002/bz020417.gif>>

Gli hacker prendono di mira Israele:

<<http://www.computing.vnunet.com/News/1130941>>

Su Slashdot si può trovare una discussione a seguito del mio articolo su "responsabilità e sicurezza":

<<http://slashdot.org/article.pl?sid=02/04/21/0058214&mode=thread>>

Un comune amministratore di rete viene sommerso da rapporti sulla sicurezza, avvisi, allarmi, ecc. Molte di queste comunicazioni sono montature che servono a lanciare un determinato prodotto o servizio.

<<http://www.newsfactor.com/perl/story/17273.html>>

<<http://www.cnn.com/2002/TECH/internet/04/24/virus.hype/index.html>>

Come Microsoft dovrebbe trattare le falle di sicurezza e come potrebbe incrementare la fiducia:

<<http://www.osopinion.com/perl/story/17344.html>>

Nuovi strumenti di hacking che aggirano firewall e IDS:

<<http://www.zdnet.it/zdnet/JumpNews.asp?idChannel=917&idNews=119433>>

<<http://www.nwfusion.com/news/2002/0415idsevad.html>>

I dipendenti potrebbero essere la minaccia più pericolosa per la sicurezza:

<<http://www.zdnet.it/zdnet/JumpNews.asp?idChannel=917&idNews=119434>>

<<http://www.computerworld.com/securitytopics/security/story/0,10801,70112,00.html>>

<[http://www.economist.com/science/tq/displaystory.cfm?story\\_id=1020715](http://www.economist.com/science/tq/displaystory.cfm?story_id=1020715)>

Ottima discussione sui documenti d'identità nazionali. Una lettura d'obbligo per chiunque sia coinvolto nel dibattito.

<[http://books.nap.edu/html/id\\_questions](http://books.nap.edu/html/id_questions)>

Una tesi a favore di un database biometrico nazionale. Non credo che l'autore capisca molto in fatto di sicurezza:

<[http://www.acm.org/ubiquity/views/j\\_carlisle\\_1.html](http://www.acm.org/ubiquity/views/j_carlisle_1.html)>

La ISS ha trasmesso degli ottimi spot televisivi sull'intrusion detection. Se ve li siete persi, è possibile vederli qui:

<<http://www.iss.net/campaigns/index.php>>

Un rapporto in tre parti sulla sicurezza delle banche in generale. La prima parte tratta dell'aumento delle falle di sicurezza, la seconda riguarda l'anatomia di un hack, e la terza è uno sguardo d'insieme ad alcune delle ragioni delle insicurezze nel sistema.

<<http://www.zdnet.it/zdnet/JumpNews.asp?idChannel=917&idNews=119435>>

Un'azienda francese, Vivendi, ha indetto una votazione elettronica. In seguito è corsa voce che alcuni hacker avessero truccato i voti. Altri hanno sostenuto che tutto era stato svolto regolarmente. Ora sono stati coinvolti i tribunali. Questo mette in risalto il problema più grande per ciò che riguarda le votazioni in forma elettronica: esse sono alterabili, e non c'è modo di dimostrare il contrario.

<<http://europe.cnn.com/2002/BUSINESS/04/29/vivendi.hacker/index.html>>

<<http://www.wired.com/news/business/0,1367,52162,00.html>>

<<http://www.silicon.com/a52986>> <<http://www.silicon.com/a53068>>

<<http://www.vnunet.com/News/1131506>>

Eccellente articolo sulla gestione dei diritti digitali e sulla protezione dalla copia:

<<http://www.reason.com/0205/fe.mg.hollywood.shtml>>

Il General Accounting Office ha pubblicato un rapporto dal titolo: "National Preparedness: Technologies to Secure Federal Buildings" ("Essere preparati a livello nazionale: tecnologie per la sicurezza degli edifici federali"). Lo scritto esamina una serie di tecnologie di sicurezza disponibili sul mercato, dalle swipe card ai sistemi biometrici.

<<http://www.gao.gov/new.items/d02687t.pdf>>

Massiccio attacco ai danni della modalità di pagamento in carta di credito attraverso Authorize.net. Vengono inseriti nel sistema dei numeri casuali, e di tanto in tanto il metodo funziona.

<<http://www.msnbc.com/news/742677.asp>>

Bell'articolo sulla realizzazione di una tassonomia delle diverse tipologie d'attacco ai network.

<<http://www.osopinion.com/perl/story/17692.html>>

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

Le News di Counterpane

Due grosse novità questo mese. La prima: Counterpane è entrata nel Red Herring 100 (ovvero l'elenco delle cento aziende giudicate maggiormente innovatrici nei loro rispettivi campi dalla rivista Red Herring):

<<http://www.counterpane.com/pr-red100.html>>

<<http://www.redherring.com/insider/2002/0513/tech-rh100.html>>

La seconda: abbiamo un nuovo accordo di distribuzione con VeriSign. VeriSign offre un portafoglio di servizi di gestione della sicurezza. Due settimane fa hanno aggiunto i servizi di monitoraggio di Counterpane a quel portafoglio. D'ora innanzi, ogni contratto di servizio venduto da VeriSign comprenderà il monitoraggio di Counterpane.

<[http://corporate.verisign.com/news/2002/pr\\_20020507.html](http://corporate.verisign.com/news/2002/pr_20020507.html)>

<<http://www.theregister.co.uk/content/55/25168.html>>

Schneier interverrà alla RSA Giappone il 29 maggio.

<<http://www.key3media.co.jp/rsa2002/eng/index.html>>

Schneier interverrà alla Infraguard conference a Cleveland il 7 giugno.

<<http://www.nocinfragard.org>>

Schneier interverrà all'annuale USENIX Conference a Monterey il 15 giugno.

Schneier interverrà al NetSec a Chicago il 18 giugno, per due volte.



Le carte di Matsumoto non sono sul Web. È possibile averne una copia facendo richiesta a Tsutomu Matsumoto stesso: <[tsutomu@mlab.jks.ynu.ac.jp](mailto:tsutomu@mlab.jks.ynu.ac.jp)>

Il riferimento è il seguente: T. Matsumoto, H. Matsumoto, K. Yamada, S.Hoshino, "Impact of Artificial Gummy Fingers on Fingerprint Systems,"

Proceedings of SPIE Vol. #4677, Optical Security and Counterfeit Deterrence Techniques IV, 2002.

Alcune diapositive della presentazione si trovano qui.

<<http://www.itu.int/itudoc/itu-t/workshop/security/present/s5p4.pdf>>

Il mio precedente articolo sull'uso e abuso della biometrica.

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

La biometrica e il centro commerciale: fare la spesa con l'impronta del pollice.

<[http://seattlepi.nwsourc.com/local/68217\\_thumb27.shtml](http://seattlepi.nwsourc.com/local/68217_thumb27.shtml)>

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

Commenti dei lettori

Da: "Joosten, H.J.M." <[H.J.M.Joosten@kpn.com](mailto:H.J.M.Joosten@kpn.com)>

Oggetto: Come ragionare in merito alla sicurezza

- > Sempre di più e sempre più spesso all'opinione pubblica viene richiesto di prendere
- > decisioni in merito alla sicurezza, di ponderare compensazioni che comprendano la
- > sicurezza, e di accettare un tipo di sicurezza sempre più intrusiva.
- > Sfortunatamente l'opinione pubblica non ha idea di come affrontare tutto questo.

La gente è di certo in grado di prendere decisioni in merito alla sicurezza. Si acquistano allarmi anti-rapina, si installano lucchetti, ci si affida alle assicurazioni continuamente. Naturalmente tutto ciò non è sempre d'aiuto, e le persone possono prendere decisioni diverse a seconda del livello di sicurezza a loro necessario, ma non vedo grosse differenze rispetto al prendere decisioni.

Allora, in che cosa consiste la differenza? Le persone nel "mondo reale" hanno un'idea di che cosa siano i problemi legati alla sicurezza. Si può subire il furto della propria auto, il proprio appartamento può essere svaligiato, e così via. Tutti sono in grado di percepire le conseguenze legate al doversi comprare un'altra automobile, al doversi ricomprare tutto ciò che è stato rubato e riparare la porta d'ingresso.

La gente non arriva ad avere quest'idea rispetto alla sicurezza informatica. Si può sentir dire: "cos'è questa storia dei settaggi del firewall? I clienti non si lamentano, e pagano. E allora QUALI sono i problemi che devo risolvere?" Le persone non sembrano accorgersi delle REALI conseguenze. All'interno delle aziende questa può essere una problematica organizzativa. Per quanto riguarda i singoli individui, non pare sussistano gravi problemi se ci si attiene a quello che il proprio ISP stabilisce come norme di buona pratica.

Noi, in qualità di esperti di sicurezza, parliamo in continuazione di quanto POSSA accadere, e siamo tutti contenti se un qualche incidente accade davvero. Molti di questi incidenti non vengono veramente percepiti dalla gente, che non li avverte come un loro problema. Noi possiamo intimidire le persone attirando l'attenzione su quegli incidenti. Ma queste persone

non hanno un problema di sicurezza. Il loro problema è legato alla paura, ed è un problema che può facilmente risolvere la stessa fonte che ha instillato la paura. Ecco come certe vendite possono funzionare e vengono fatte funzionare nell'ambito della sicurezza.

Perciò, mentre il suo "punto primo - che tipo di problemi risolve una misura di sicurezza?" è un passo cruciale, c'è ancora molto lavoro da fare prima di esso. Occorrerebbe trovare un metodo di "auto-aiuto" per il grande pubblico, in modo che possa venire utilizzato per far fronte ai vari problemi che le persone percepiscono davvero dal loro punto di vista. In questo modo esse diventano responsabili, nel senso che quando le cose diventeranno spiacevoli saranno le stesse persone a doverne affrontare le conseguenze. Nei casi in cui non si percepiscono vere e proprie conseguenze, non si hanno problemi. Se svaligiano casa vostra, o quella del vostro vicino, o una casa nelle vostre vicinanze, ecco che il problema viene percepito, e ci si appresta a fare qualcosa per risolverlo. La gente può fare questo. Lo ha sempre fatto. Allora, e solo allora, la sua analisi in cinque punti potrà essere d'aiuto.

Da: "John Sforza" <[jsforza@isrisk.net](mailto:jsforza@isrisk.net)>

Oggetto: Come ragionare in merito alla sicurezza

Concordo sul fatto che il grande pubblico (di questi tempi) non abbia molta esperienza nel prendere decisioni sulla sicurezza in merito a infrastrutture, informazioni e problematiche di privacy che siano informate ed intelligenti. Non sono affatto d'accordo, tuttavia, sul fatto che chi opera nell'ambito della sicurezza informatica sia migliore nel prendere queste decisioni soltanto perché si trova a far fronte a queste problematiche continuamente. Sarei molto più colpito dalla competenza della comunità per la sicurezza informatica se vi fosse una qualche indicazione che dimostri ottimi risultati derivanti dalla loro attività.

Mi figuro l'industria della sicurezza informatica come un gruppo di bimbi dispersi nella foresta quando si tratta di andare al di là dei propri computer, del proprio software e fuori dal proprio ambito. Le professioni di operazioni di intelligence, operazioni di sicurezza, di counter intelligence, e di semplice spionaggio hanno alle spalle movimentate decadi di esperienza e secoli di storia operativa. Siete voi ad essere le nuove leve che cercano di applicare le migliori norme dettate dalla storia di queste discipline nell'ambito della cosiddetta sicurezza informatica, vantando meriti intellettuali. In generale, la comunità della sicurezza informatica è - in termini di esperienza - vecchia di nemmeno 15 anni, e la maggior parte di essa non ha più di dieci anni di esperienza in cose che vadano oltre le ACL, le password e la crittografia di base. Quasi nessuno di questa comunità ha un minimo background in physical security, operazioni di copertura, contesto culturale in riferimento alla sicurezza, o mera esperienza diretta, nel mondo reale, al di là dei propri piccoli uffici.

Ho anche notato come in genere coloro che lavorano nella sicurezza informatica si rivelino pessimi istruttori per il grande pubblico; ciò è dovuto soprattutto a ristrettezza di vedute, arroganza tecnica, e una basilare incapacità nel comprendere il processo di apprendimento. Solo perché si è esperti in un campo, non si deve presumere di avere capacità valide per tutto.

Infine, se da un lato i suoi cinque punti sono ottime norme di buona pratica (vecchie di secoli e documentate), dall'altro non si possono definire infallibili in alcun modo formale. In altre parole: se fosse così semplice, perché i vostri cosiddetti esperti sono così carichi di lavoro nel vostro stesso campo?

Le sue affermazioni continuano a promuovere il più grande problema di sicurezza generale che ci troviamo ad affrontare: dilettanti entusiasti muniti di certificati, a cui viene detto di essere i migliori.

Da: "John.Deters" <[John.Deters@target.com](mailto:John.Deters@target.com)>  
Oggetto: Come ragionare in merito alla sicurezza

Molta della sicurezza è in primo luogo emotiva e psicologica, come dimostra quanto è accaduto dopo gli attacchi dell'11 settembre. I mercati azionari, il turismo, e tutte quelle industrie che hanno accusato il colpo, stanno facendo affidamento sulla totalità di queste misure di sicurezza, compresi i palliativi, per riprendersi. Per chi si intende di sicurezza questo può sembrare un castello di carte o una mera operazione di abbellimento, ma la maggior parte della gente non si intende di sicurezza. Ha bisogno di vedere "qualcuno fare qualcosa", perché la grande realtà di quella tragedia è andata oltre il pensiero razionale.

Detto questo, aggiungerei che molto di ciò che lei definisce "palliativo" produce davvero un effetto positivo e tangibile sulla nazione e sull'economia.

È reale la ripresa? Devo rispondere di sì. La gente ha ripreso a volare. I mercati azionari stanno lentamente riprendendo quota. Anche se la ripresa del mercato è costruita su un castello di carte, o sulla sicurezza "virtuale" prodotta dal Patriot Act o dalle truppe della guardia nazionale presenti negli aeroporti, tutto concorre a ripristinare fiducia.

Perciò tutto questo vuol forse dire che Natale è arrivato in anticipo per quei ciarlatani venditori di rimedi miracolosi? Sì. Si deve forse smettere patriotticamente di far presente la verità in merito a queste pratiche, dicendo che sono tutte montature? Naturalmente no. La vera sicurezza è ancora una meta nobile e desiderabile, e tutti sappiamo come la falsa sicurezza contemporaneamente nasconda le vulnerabilità e apra nuovi canali per effettuare attacchi. Ciò che intendo dire è che tutti abbiamo bisogno di comprendere l'intero sistema che è il nostro mondo, molto del quale è guidato in maniera emotiva e soggettiva da persone che non hanno mai sentito parlare di crittografia, o che pensano che l'essere sicuri sia rappresentato da una bomboletta spray fissata alla cintura del tizio della sicurezza all'aeroporto. Si pensi a quanto più lentamente la nazione potrebbe ritrovare fiducia se si implementassero solo ed unicamente le poche contromisure atte ad un vero incremento della sicurezza.

Da: <[nemo@cise.ufl.edu](mailto:nemo@cise.ufl.edu)>  
Oggetto: Responsabilità e sicurezza

In riferimento al suo articolo sulla "responsabilità e sicurezza", ammetto di essere d'accordo con lei per molti aspetti, con un'unica fondamentale eccezione. Dopo essermi a lungo soffermato su quegli stessi punti, sono giunto alla conclusione che non è nemmeno necessaria l'esistenza del primo punto (legislazione in merito alla responsabilità) per permettere l'esistenza del secondo (sicurezza guidata dall'industria assicurativa). Infatti, data l'estrema evidenza dell'ignoranza dei nostri legislatori in merito alla sicurezza, unita all'influenza dei rivenditori più potenti nel medesimo ambito, potrebbe essere un bene che non esistano ancora delle leggi appropriate (una causa legale per responsabilità civile potrebbe essere un buon approccio per fare della retorica).

D'altra parte mi è impossibile immaginare che qualsiasi rivenditore possa convincere una compagnia di assicurazioni ad abbassare le tariffe ai suoi clienti nel caso in cui i suoi prodotti non siano di qualità. L'assicuratore è guidato dal proprio punto di vista sul valore previsto, prospettiva basata sullo storico delle prestazioni precedenti, e stabilisce quindi le tariffe e le categorie del premio in base alle sue stime migliori e al suo desiderio di profitto. Se non è vantaggioso farlo, allora non lo farà. Non m'importa davvero se un rivenditore paga un assicuratore per garantire un momento di tranquillità ai clienti se essi utilizzano il prodotto del rivenditore, perché questo va a tutto vantaggio del rivenditore, come del resto le vendite ribassate (da clienti che non comprano prodotti troppo cari da assicurare), ma all'estremo opposto. Il rivenditore dovrà fare in modo che convenga economicamente all'assicuratore modificare i tassi, in modo che la "bustarella" dovrà rimanere comunque "onesta". Quando

costa meno realizzare buoni prodotti piuttosto che pagare per sistemarli e per i danni che causano (o sovvenzionare terze parti allo scopo), allora il rivenditore andrà in quella direzione.

Per far sì che un cliente acquisti un'assicurazione (e fare in modo che l'industria assicurativa guidi la sicurezza), egli deve avere un incentivo. Questo incentivo dovrà provenire dalla responsabilità, ma dev'essere responsabilità di tipo civile - non del rivenditore direttamente, ma dell'azienda che si serve dei prodotti di quel rivenditore. Tutto ciò avrà probabilmente le sue conseguenze per gli acquirenti di software istituzionale, ma sarà comunque sufficiente.

In una sorta di visione ideale di tutto questo, gli assicuratori si comportano come le reti di Bayes, offrendo informazioni (parziali) sul reale Costo Totale di Possesso (TCO) di un prodotto. In questo caso il TCO è composto da: costo iniziale (prezzo di vendita del software più le esercitazioni), costo di utilizzo (difficile da quantificare, si tratta del costo quotidiano di utilizzo del prodotto in termini di interoperabilità, interfaccia utente, ecc.), costo di mantenimento (mantenere il prodotto in funzione, aggiornarlo, adattarlo a nuovi utenti e a nuove configurazioni), e costo legato alla responsabilità (l'assicurazione). Attualmente l'ultimo elemento viene trascurato la maggior parte delle volte. Anche i due elementi di mezzo vengono solo ora presi in tutta la considerazione che meritano, e sospetto che esista un forte "effetto ricompensa" sui benefici d'uso al variare del numero di clienti che si serve di un determinato software (il "fattore Betamax"). Quest'ultimo aspetto può fornire robusti incentivi ai rivenditori affinché non perdano quote di mercato, il che può amplificare l'effetto sortito dalla presenza di strutture assicurative.

Da: "John Brooks" <[john\\_g\\_brooks@hotmail.com](mailto:john_g_brooks@hotmail.com)>  
Oggetto: Responsabilità e sicurezza

Spingere la gestione dei rischi in direzione delle compagnie assicurative comporta due grossi problemi.

Primo - l'intrinseco spirito conservatore dell'industria assicurativa. Può volerci molto tempo prima che muova la sua attenzione collettiva verso nuovi scenari. Nel frattempo essa accetta di buon grado il denaro proveniente da clienti volontari, ma la copertura fornita può non avere molto valore. Per esempio, prendiamo l' "assicurazione sui dati" qui nel Regno Unito. È da molto tempo che si trova in circolazione e ha la pretesa di coprire tutti i rischi (o almeno la maggior parte di essi). Ma per moltissimo tempo il valore effettivo dei dati è stato calcolato in modi alquanto bizzarri e non esisteva ALCUNA copertura contro i problemi e i costi aggiuntivi derivati dall'impossibilità di avere accesso ai dati stessi! Mi auguro che questa situazione sia migliorata ultimamente, con più enti assicurativi entranti nel mercato.

Secondo - gli effetti del monopolio. Nel Regno Unito esistono un paio di "organizzazioni commerciali" vicine all'industria assicurativa, con soci che si occupano di installazione di sistemi di physical security (ad es. NACOSS). Senza dubbio queste "associazioni" hanno un certo valore, ma molte di queste cose sembrano fatte più per i propri soci che per gli utenti di un sistema di sicurezza. Mi si perdoni il cinismo - ma qui stiamo parlando di natura umana. Qualsiasi organizzazione che abbia un'esclusività basata sull'insieme dei soci o altri simili meccanismi può creare "influenze negative" sull'industria o sul gruppo o gruppi di interesse che dovrebbe aiutare. Eventuali parallelismi con i gruppi industriali musicali, per la maggior parte statunitensi (RIAA, ecc.), risultano ovvi.

Non ho nulla contro le assicurazioni. È la qualità dell'analisi dei rischi e il numero dei luoghi in cui viene fatta (più d'uno, si spera!) a seccarmi. Inoltre dovremmo tutti ricordare che la "direttiva primaria" di qualsiasi compagnia assicurativa è "se è possibile, non sborsare denaro!"

Da: Glenn Pure <[Glenn.Pure@pcug.org.au](mailto:Glenn.Pure@pcug.org.au)>  
Oggetto: Responsabilità e sicurezza

Sono completamente d'accordo con lei quando sostiene che l'industria del software dovrebbe essere ritenuta responsabile per i difetti nei propri prodotti come ogni altra industria. Allo stesso tempo, vincere una causa per danni dovuti ad un'imperfetta funzione di sicurezza può essere assai difficile in molti casi, a causa della difficoltà nello stabilire il grado in cui un difetto del software ha contribuito alla perdita generale (se comparato alla mole di problemi legati a software, configurazioni, architetture, management o personale).

Ma, ancor peggio, credo che la responsabilità non funzionerà affatto. Rendere le aziende produttrici di software responsabili darà loro unicamente un incentivo per stilare accordi di licenza ancora più furbi in modo che siano esenti da ogni responsabilità. Se crede che questo mio commento sia dettato dal cinismo, in realtà non lo è. Si tratta di semplice logica. Un produttore di software che dovesse affrontare la prospettiva di veder saltare i costi della produzione di software e i tempi dedicati allo sviluppo, cercherà delle alternative per ridurre la propria responsabilità. Sono sicuro che le menti eccelse di quest'industria troveranno moltissime idee più a buon mercato (che evitano l'assai costoso iter di sistemare il problema efficacemente), compresa una revisione "creativa" dei termini di licenza.

Allo stesso modo i compratori di software non saranno più molto convinti nell'acquistare prodotti migliori per la sicurezza (o prodotti con migliori misure in termini di responsabilità) se, come lei stesso afferma chiaramente, non gliene importa molto fin dal principio. Nella misura in cui a loro importa, non dormiranno certo sonni più tranquilli sapendo che possono denunciare un'azienda negligente per un baco della sicurezza. Sarebbe come dire che la rigorosa manutenzione delle linee aeree commerciali e i relativi controlli di sicurezza non servono più se si dispone un buon paracadute sotto il sedile di ogni passeggero!

Da: <[jja@lusArs.net](mailto:jja@lusArs.net)>  
Oggetto: Responsabilità e sicurezza

Credo che lei stia decantando le meraviglie della responsabilità in maniera eccessiva, e in molti modi. Anzitutto non sta tenendo in considerazione i costi della responsabilità. Le compagnie potrebbero andare in fallimento non per causa loro, ma perché un giudice o una giuria non sono stati in grado di comprendere correttamente la situazione che ha scatenato la causa legale. Brave persone perderanno il loro posto di lavoro, e buoni prodotti verranno tolti dal mercato. Un'assicurazione può ridurre il problema, ma non lo eliminerà. Buoni prodotti, realizzati da individui che hanno la sfortuna di non conoscere le persone giuste, verranno ignorati, perché le compagnie assicurative non li valuteranno nemmeno. Gli indennizzi verranno stabiliti da giurie totalmente sproporzionate rispetto agli eventi che staranno condannando. E questo è solo l'inizio.

In secondo luogo lei non tiene in conto che le compagnie assicurative troppo spesso sono talmente lente nel reagire che l'industria della sicurezza in ambito tradizionale è in gran parte una buffonata. La sicurezza per loro non è il fermare determinate persone, e nemmeno lo scoprirle. È semplicemente questione di far quadrare il bilancio. Ed è quello che sta accadendo anche oggi, solo che diverse persone stanno pagandone il prezzo in vari modi. La responsabilità può essere (e io credo che sia) un modello migliore, in media, ma non è necessariamente "più sicuro" da un punto di vista tecnico, ed è molto ingenuo affermare il contrario. I servizi di una compagnia possono ridurre i tassi assicurativi, ma è altresì probabile che anche metodi più semplici, più stupidi e meno efficaci portino allo stesso risultato, e il rapporto costi/benefici potrebbero rivelarsi vicini o meno alle aspettative. Ricordiamoci che anche le compagnie assicurative affrontano un costo di compensazione: determinare quali misure funzionano e quanto bene esse debbano funzionare, e chiedere alle persone di pagare anticipatamente una certa cifra per ridurre i tassi assicurativi, sono costi. Quindi esse si limitano a fare bene questo e nient'altro - anche a discapito della competitività rispetto ad altre compagnie assicurative. Dato il pessimo stato delle strutture di sicurezza che vengono fatte assicurare, è ovvio quanto imperfetto sia tutto questo meccanismo.

Credo davvero che la sicurezza basata sulla responsabilità sia un'ottima cosa, ma non è una panacea. Tutti sappiamo che nulla è perfetto, e che nessuno si aspetta che lo sia.

Da: Todd Owen <[towen@lucidcalm.dropbear.id.au](mailto:towen@lucidcalm.dropbear.id.au)>

Oggetto: Responsabilità e sicurezza

Le sue argomentazioni in merito all'imposizione di responsabilità legali sul software sono molto interessanti, e sono sicuramente d'accordo sul fatto che la causa principale del software non sicuro non è una problematica tecnologica. Ma varrebbe forse la pena notare come ciò che lei suggerisce vada ad applicarsi solo ad un certo tipo di società, cioè il nostro modello occidentale, e al sistema economico corporativo / capitalistico.

Il problema (come lei ha già dimostrato) non è che le aziende non possano migliorare la sicurezza dei propri prodotti, è che non vogliono farlo. I dirigenti non hanno voglia di perdere tempo e denaro migliorando la sicurezza, da un lato a causa delle pressioni del mercato, e dall'altro perché la cultura corporativa insegna loro il mantra "massimizzare i profitti" a scapito di qualsiasi altra cosa. Naturalmente la sicurezza non è l'unica vittima di questo modo di pensare (chiamato anche "razionalismo economico"). Questa metodologia aziendale giustifica anche la grande quantità di inquinamento e distruzione ambientale, nonché un trattamento degli impiegati (specie nei paesi del Terzo Mondo) scarsamente etico ed altri comportamenti poco etici o illegali, come la falsa pubblicità e il controllo da parte del potere monopolistico.

Vengono utilizzate diverse contromisure per contrastare queste problematiche, ed esse variano dal sindacalismo alla legislazione. Se la responsabilità potesse rispondere al problema della qualità del software, allora sarebbe la soluzione di cui abbiamo bisogno.

Tuttavia credo che Greg Guerin (cfr. Crypto-Gram - gennaio 2002) abbia ragione ad essere preoccupato per quanto riguarda il peso della responsabilità nel caso di piccole aziende o del software open source. L'effetto della responsabilità (e dell'assicurazione) in questi casi dipenderebbe da come esattamente venisse legiferata la responsabilità. Ma se tutto questo finisse con lo svantaggiare il software open source, allora troverei la cosa tristemente ironica, perché il Free Software movement è in parte una risposta alla mentalità corporativa dell' "avidità a tutti i costi" che mi pare essere la causa principale del problema della qualità del software.

Un altro aspetto da considerare è che la responsabilità legata al software potrebbe incoraggiare la "mentalità litigiosa" del mondo moderno (soprattutto negli USA). Assisteremo ad opportunistiche cause legali che riterranno responsabile il produttore di un software in caso di intrusione in un network anche se la password di root era proprio "password"?

Penso che, a lungo andare, una mossa mirata ad incoraggiare le aziende a prendersi davvero cura dei propri clienti (invece che curarsi solo del profitto) potrebbe rivelarsi più utile, invece di costringerle ad aumentare la qualità attraverso misure legali. Ma questo richiederebbe molto più che del lobbismo politico per arrivare ad un risultato.

Da: "Tousley, Scott W." <[Scott.Tousley@anser.org](mailto:Scott.Tousley@anser.org)>

Oggetto: Il rapporto "2002 CSI/FBI Computer Crime Survey"

Credo che il rapporto di quest'anno prosegua l'allontanamento da una forma di compendio di risposte effettive, spingendosi sempre più verso una pubblica difesa dei problemi. Questa difesa è presentata in maniera così forte che il lettore neutrale inizia ben presto a mettere da parte questo "rapporto" come un qualsiasi oggetto sponsorizzato di marketing.

Ancora una volta sono estremamente deluso nel non vedere alcuno sforzo per normalizzare l'attività criminale e illecita contro le tendenze di fondo dell'attività economica, del commercio elettronico, ecc. Continuo a leggere i vari "studi" del CSI come indicazioni di un livello relativamente costante di attività illecita, ove la crescita apparente riportata nei bollettini è

quasi totalmente proporzionale alla (e spiegata dalla) sempre maggiore presenza di attività economica legata al network, alla sempre maggiore consapevolezza delle problematiche legate alla sicurezza informatica, ecc. Ritengo che il CSI stia perdendo una grossa opportunità a questo punto, perché se ridefinisse la linea di base delle informazioni escludendo il fattore background, allora potrebbe riferirsi alle possibili tendenze in maniera più obiettiva e con maggiore credibilità rispetto al lettore neutrale. Questo sforzo sostenuto da parte del CSI ha il vantaggio di individuare per primo queste tendenze commerciali d'impatto, e mi spiacerebbe vederlo sprecato in una perdita di qualità e di attenzione per quanto concerne le informazioni più importanti.

Da: David Haworth <[david.haworth@altavista.net](mailto:david.haworth@altavista.net)>  
Oggetto: CBDTPA

In tutti gli articoli che ho letto e che criticano il CBDTPA, non ho mai visto nessuno scrivere in merito a una delle sue conseguenze: esso potrebbe mettere gli USA in condizione di violare i trattati WIPO che sono stati implementati molto attentamente e fin troppo esaustivamente insieme al DMCA.

Negli "Agreed Statements" (dichiarazioni convenute) in coda all'articolo 12 del WIPO copyright treaty (l'articolo che richiede provvedimenti legali contro la rimozione di informazioni che riguardano la gestione dei diritti digitali), si legge chiaramente:

"È inoltre stabilito che le parti contraenti non faranno affidamento sul presente articolo per disporre o implementare sistemi di amministrazione dei diritti che avrebbero l'effetto di imporre formalità non permesse sotto la Convenzione di Berna o da questo Trattato, proibendo la libera circolazione delle merci o impedendo il godimento dei diritti sotto il presente Trattato."

Il CBDTPA, insieme al brevetto DRM-OS di Microsoft e senza dubbio a un'enorme quantità di altri brevetti software che non incorrono in restrizioni al di fuori degli Stati Uniti, non sarebbero altro che quella barriera alla libera circolazione delle merci che gli Stati Uniti, in pieno accordo con la dichiarazione di cui sopra, si erano impegnati a non creare.

Da: <[kragen@pobox.com](mailto:kragen@pobox.com)> (Kragen Sitaker)  
Oggetto: Vulnerabilità del protocollo SNMP

Nel numero di aprile di Crypto-Gram, Bancroft Scott scrisse:

- > Se le applicazioni che usano ASN.1 vengono propriamente implementate e testate,
- > esse risultano essere sicure come qualsiasi altro programma debitamente
- > implementato e verificato.

Se con "debitamente implementato" si intende "corretto", allora questa affermazione è, con ogni probabilità, oziosamente vera; sarei davvero sorpreso se esistessero programmi sufficientemente complessi da usare ASN.1 che fossero liberi da bug.

Se, d'altra parte, si intende "implementato secondo le attuali migliori norme di programmazione", allora l'affermazione è ancora una volta, con ogni probabilità, oziosamente vera. Le attuali migliori norme di programmazione sono probabilmente quelle messe in pratica dal team software a bordo dello shuttle, che ha un tasso di errore pari a un bug per 10.000 righe di codice; il costo del team è dell'ordine del milione di dollari (moltiplicato o diviso per



