

problema, secondo questa posizione, riguarda l'informazione in merito a una vulnerabilità più che la vulnerabilità stessa.

Questa posizione ignora il fatto che un attento esame a livello pubblico è l'unico sistema affidabile per migliorare la sicurezza. Vi sono parecchi sistemi a passe-partout che sono immuni all'attacco "ultracentenario" che è stato riscoperto da Blaze. Non sono molto comuni sul mercato, in primis perché gli acquirenti non comprendono i rischi legati alla sicurezza, e poi perché i fabbrici continuano a vendere volontariamente un sistema di sicurezza fallato piuttosto che ammettere l'esistenza del problema e poi risolverlo. Questo non è affatto diverso da ciò che accade in campo informatico. Prima che le vulnerabilità dei software venissero pubblicate periodicamente, i produttori non si sarebbero certo preoccupati di investire tempo e denaro per sistemarle, confidando nella sicurezza della segretezza. Dato che gli acquirenti non erano a conoscenza del problema, essi compravano questi sistemi ritenendoli sicuri. Se in ambito informatico dovessimo ritornare in un mondo dominato dalla segretezza sui bug, avremmo l'equivalente di centenarie vulnerabilità note solo a poche persone della comunità per la sicurezza e alla comunità degli hacker.

Questa è l'altra convinzione sbagliata riguardante la posizione dei fabbrici. Tecniche come questa sono state trasmesse come folklore sia dalla comunità criminale che da quella dei fabbrici. Nel 1994 un ladro si costruì un passe-partout per aprire una serie di cassette di sicurezza e rubò gioielli per un valore di un miliardo e mezzo di dollari. La stessa cosa accade nel mondo informatico. Quando una vulnerabilità software viene annunciata dalla stampa e viene poi sistemata, essa è già folklore nel sottobosco degli hacker. Gli attaccanti non rispettano accordi sulla segretezza.

Quello a cui stiamo assistendo è un conflitto culturale; sta accadendo in vari ambiti della sicurezza. Il ministro della giustizia Ashcroft è all'opera per mantenere segreti i dettagli di svariate contromisure antiterrorismo in modo da non permettere ai terroristi di informarsi. Ma allo stesso tempo all'opinione pubblica -- a cui egli in definitiva deve render conto -- non è permesso valutare quelle stesse contromisure, né commentarne l'efficacia. In assenza di un dibattito e di un'educazione a livello pubblico, la sicurezza non può migliorare. Ogni attacco ed ogni difesa appresi dalle persone diverrebbero note di folklore, mai discussi in pubblico ma sussurrati fra ingegneri della sicurezza da una parte e fra terroristi dall'altra. Forse dopo cent'anni qualcuno pubblicherà un attacco noto ad alcuni ingegneri, sempre sfruttato da criminali e terroristi, ma del quale l'opinione pubblica è sempre stata ignara.

La segretezza impedisce alle persone dal valutare i loro stessi rischi. Per esempio, nel caso del passe-partout, anche se non vi fossero disponibili modelli più sicuri, molti acquirenti avrebbero potuto decidere di non utilizzare il sistema a passe-partout se avessero saputo quanto è semplice, per un assalitore, costruirsi il proprio passe-partout.

Preferirei avere più informazioni possibili in modo da poter prendere una decisione consapevole in merito alla sicurezza. Preferirei essere in possesso delle informazioni di cui ho bisogno così da costringere i produttori e i rivenditori a migliorare la sicurezza. Non voglio vivere in un mondo dove dei fabbrici possono vendermi un sistema a passe-partout che sanno bene non funzionare, o dove il governo può attuare delle misure di sicurezza senza doverne rendere conto a nessuno.

La home page della ricerca di Blaze:

<<http://www.crypto.com/masterkey.html>>

Lo studio:

<<http://www.crypto.com/papers/mk.pdf>>

Le reazioni allo studio:

<<http://www.crypto.com/papers/kiss.html>>

Nuovi articoli sulla ricerca:

<<http://www.nytimes.com/2003/01/23/business/23LOCK.html>>

<<http://www.mail-archive.com/cryptography@wasabisystems.com/msg03415.html>>

Precedenti riferimenti alla tecnica di Blaze:

<<http://sethf.com/infthought/blog/archives/000164.html>>

Il furto di gioielli che ha sfruttato la vulnerabilità del passe-partout:

<<http://www.nbc4columbus.com/news/1921563/detail.html>>

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

Le ristampe di Crypto-Gram

Crypto-Gram è attualmente al suo sesto anno di pubblicazione. I numeri precedenti coprono tutta una serie di argomenti legati alla sicurezza e si possono trovare 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.

Microsoft e il "trustworthy computing":

<<http://www.counterpane.com./crypto-gram-0202.html#1>> (originale)

<<http://www.cryptogram.it/febbraio02.htm#a1>> (traduzione in italiano)

Considerazioni su Microsoft:

<<http://www.counterpane.com./crypto-gram-0202.html#2>> (originale)

<<http://www.cryptogram.it/febbraio02.htm#a2>> (traduzione in italiano)

Protezione anti-copia incorporata negli hard disk:

<<http://www.counterpane.com/crypto-gram-0102.html#1>>

Un attacco semantico sugli URL:

<<http://www.counterpane.com/crypto-gram-0102.html#7>>

L'idiozia dei filtri e-mail:

<<http://www.counterpane.com/crypto-gram-0102.html#8>>

Gli air gaps:

<<http://www.counterpane.com/crypto-gram-0102.html#9>>

Il voto in Internet di contro all'e-commerce su vasta scala:

<<http://www.counterpane.com/crypto-gram-0102.html#10>>

Attacchi denial-of-service distribuiti:

<<http://www.counterpane.com/crypto-gram-0002.html#DistributedDenial-of-ServiceAttacks>>

Riconoscere i metodi fasulli in ambito crittografico:

<<http://www.counterpane.com/crypto-gram-9902.html#snakeoil>>

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

Note sparse sul worm SQL Slammer

Internet ha recentemente avuto un'altra grande epidemia dopo il virus Nimda: il worm Sapphire, detto anche SQL Slammer. Di solito non mi preoccuperei nemmeno di menzionare un simile worm. È una novità, ma non vi sono lezioni da imparare da questo evento. Però c'è un interessante colpo di scena da parte di Microsoft. Durante i giorni dell'attacco, Microsoft ha cercato di deviare ogni accusa dichiarando di aver prodotto una patch per questa vulnerabilità sei mesi prima, e che le sole compagnie affette dal virus erano quelle che non avevano mantenuto aggiornate le patch. Un paio di giorni dopo si è saputo che la stessa rete di Microsoft era stata pesantemente colpita dal worm perché Microsoft stessa non l'aveva aggiornata.

Ormai sono due anni che vado ripetendo che l'idea secondo cui sia possibile ottenere la sicurezza delle reti scovando vulnerabilità e applicandovi patch "sul campo" è fatalmente sbagliata. Non biasimo gli amministratori di sistema di Microsoft per non aver mantenuto aggiornate le loro patch -- nessuno lo fa -- ma non mi piace l'ipocrisia che trasuda da quell'azienda.

Il worm SQL Slammer ha poi riaperto il dibattito sull'esposizione totale. Microsoft annunciò la vulnerabilità nel luglio 2002, nello stesso periodo in cui rilasciava la patch. Alcuni giorni dopo, David Litchfield pubblicò un codice di exploit che dimostrava come la vulnerabilità potesse essere usata per introdursi nei vari sistemi. Il worm SQL Slammer uscito a gennaio ha usato quello stesso codice. Alcuni, in base a questo, sostengono che Litchfield non avrebbe dovuto pubblicare il codice, mentre altri, più correttamente, ritengono che il codice non sia stato poi così difficile da scrivere, e che quindi l'autore del worm poteva benissimo averlo scritto per proprio conto.

Un episodio divertente, anche se non pertinente: una settimana dopo l'uscita del worm, sono stato invitato dalla CNN a parlarne in diretta televisiva. Il programma è stato poi cancellato a causa della tragedia dello Shuttle, ma non prima che i produttori della CNN invitassero Microsoft ad apparire in trasmissione insieme a me. Il portavoce di Microsoft -- non saprei chi -- ha dichiarato che la compagnia non aveva intenzione di apparire alla CNN con me. Sarebbe intervenuta prima di me, dopo di me, ma non insieme a me. Pare che sia ormai parte della condotta ufficiale di Microsoft non comparire in pubblico insieme a Bruce Schneier.

Il miglior resoconto tecnico sul worm e su come si sia propagato (davvero un'ottima lettura):
<<http://www.silicondefense.com/research/sapphire/>>

I problemi interni di Microsoft a causa del worm:

<<http://www.theregister.co.uk/content/56/29073.html>>

<<http://news.com.com/2100-1001-982305.html>>

<<http://www.cnn.com/2003/TECH/biztech/01/28/microsoft.worm.ap/>>

<<http://www.nytimes.com/2003/01/28/technology/28SOFT.html>>

Il mio studio di due anni fa sul difficile lavoro delle patch:

<<http://www.counterpane.com./crypto-gram-0103.html#1>>

L'allarme sulla sicurezza originariamente dato da Microsoft:

<<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms02-039.asp>>

oppure <<http://tinyurl.com/vel>>

I commenti di Litchfield sulle somiglianze fra il suo codice e il worm:

<<http://groups.google.com/groups?selm=b19f28%2411oo%241%40FreeBSD.csie.NCTU.edu.tw&oe=utf-8&output=gplain>>

oppure <<http://tinyurl.com/5qo6>>

<<http://sfgate.com/cgi-bin/article.cgi?f=/news/archive/2003/01/15/national1617EST0765.DTL>> oppure <<http://tinyurl.com/4i4l>>

Studio di Whitfield Diffie sul rapporto fra apertura mentale e sicurezza:
<<http://news.com.com/2010-1071-980462.html>>

La ACLU ha appena pubblicato una nuova relazione, "Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society." ("Un nemico più grande, catene più deboli: la crescita di una società di sorveglianza americana").
<<http://www.aclu.org/Privacy/Privacylist.cfm?c=39>>

Molti modem Sprint DSL sono configurati con la password "1234":
<<http://www.wired.com/news/infostructure/0,1377,57342,00.html>>

Chiunque può ottenere il proprio dominio .mil:
<<http://212.100.234.54/content/55/29026.html>>

Un'azienda produttrice di comandi automatici per l'apertura delle saracinesche dei garage sta usando il DMCA per bloccare la distribuzione di un prodotto concorrente:
<<http://www.extremetech.com/article2/0,3973,842083,00.asp>>

Questo rapporto sulle minacce di sicurezza in Internet (Internet Security Threat Report) è zeppo di statistiche ed informazioni interessanti, e ne consiglio la lettura. (Symantec richiede l'inserimento di alcuni dati personali prima di poter scaricare il rapporto, presumibilmente per vendervi i propri prodotti, ma potete sempre inserire false informazioni nel form).
<<http://enterprisecurity.symantec.com/Content.cfm?articleID=1964&EID=0>>
oppure <<http://tinyurl.com/5qoq>>

Consigli per implementare la crittografia nei sistemi:
<http://www.cs.auckland.ac.nz/~pgut001/pubs/crypto_guide.txt>

Richard Clarke sta lasciando la carica di "zar della sicurezza" alla Casa Bianca, e Howard Schmidt lo sostituirà. L'articolo seguente parla nuovamente di quelle voci secondo cui la presa di posizione di Clarke in merito alla protezione della privacy l'abbia messo in disaccordo con l'amministrazione Bush.
<<http://www.washingtonpost.com/wp-dyn/articles/A6320-2003Jan31.html>>

Buon articolo sulle responsabilità legate al software:
<<http://www.bos.frb.org/economic/nerr/rr2002/q3/perspective.pdf>>

Il Consiglio del Senato sulla Sicurezza e Difesa Nazionale in Canada ha recentemente pubblicato un rapporto sulle nuove misure di sicurezza aeroportuali. È saggio e ben scritto, a differenza di molti altri rapporti sulla sicurezza che ho avuto occasione di leggere.
<<http://www.parl.gc.ca/37/2/parlbus/commbus/senate/com-e/defe-e/rep-e/rep05jan03-e.htm>>
oppure <<http://tinyurl.com/5tzk>>

Il compratore non si fida del venditore, allora si serve di un garante per proteggersi dalle frodi. Ma che cosa può accadere se il garante è poco attendibile?
<<http://www.msnbc.com/news/854552.asp?0cl=cR>>

Gli avvocati come minaccia per la sicurezza informatica:
<<http://www.osopinion.com/perl/story/20581.html>>

Interessante intervista a Kevin Mitnick:

<<http://interviews.slashdot.org/article.pl?sid=03/02/04/2233250&mode=thread&tid=103&tid=123&tid=172>> oppure <<http://tinyurl.com/5fum>>

L'esercito statunitense sta sviluppando regole in merito alla guerra cibernetica:

<<http://www.vnunet.com/News/1138573>>
<<http://www.washingtonpost.com/wp-dyn/articles/A38110-2003Feb6.html>>
<http://www.gcn.com/vol1_no1/daily-updates/21122-1.html>

Inviare i vostri suggerimenti per il concorso sulla "più stupida misura di sicurezza a livello mondiale". Verranno assegnati dei premi.

<<http://www.privacyinternational.org/activities/stupidsecurity>>
<<http://www.theregister.co.uk/content/55/29279.html>>

Un buon articolo sui pericoli inerenti al furto di identità, e spunti su come risolvere il problema:

<http://www.businessweek.com/technology/content/feb2003/tc20030211_7896_tc047.htm> oppure <<http://tinyurl.com/5u0a>>

Questioni forensi riguardo a Windows:

<<http://online.securityfocus.com/infocus/1661>>
<<http://online.securityfocus.com/infocus/1665>>

Interessante caso di estorsione cibernetica. L'ignaro utente visita un sito web. Il server web scarica dei file nel computer della vittima. Il proprietario del server invia alla vittima un'e-mail, comunicandogli che sul suo computer c'è del materiale pornografico pedofilo e che informerà le varie autorità competenti se la vittima non paga.

<<http://www.csoonline.com/read/020103/undercover.html>>

** **

Le news di Counterpane

Sulla scia del finanziamento di 20 milioni di dollari, Counterpane ha annunciato due nuove aggiunte al team direttivo: Paul Stich in qualità di Presidente e COO, e Rahoul Seth in qualità di CFO. Tom Rowley rimane al comando in qualità di CEO.

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

** **

Note di sicurezza da ogni dove: la sicurezza anti-frode nelle banche

Le banche di solito non verificano le firme su assegni e addebiti in carta di credito. Esse, al contrario, confidano nel cliente per l'eventuale notifica di transazioni fraudolente, in modo da poter investigare di conseguenza. La banca presume che i debiti siano corretti a meno che il cliente non reclami. Nell'insieme i costi possono essere maggiori per tutti i clienti, dato che tocca a loro effettuare i controlli; ma così facendo la banca riduce i propri costi proprio perché si affida all'operato dei clienti. Anche se la banca dovrebbe agire nell'interesse del cliente, ha così scelto una soluzione di sicurezza che si rivela più costosa in termini di tempo e seccature per il cliente.

** **

L'importanza dell'autenticazione

L'autenticazione è più importante della crittografia. L'intuito di molte persone in merito alla sicurezza porta a pensare all'esatto opposto, eppure è vero. Immaginiamo una situazione in cui Alice e Bob stiano usando un canale di comunicazione sicuro per scambiarsi dati. Consideriamo quanti danni un'intercettatore potrebbe fare se potesse leggere l'intero traffico di dati. Pensiamo poi a quanti danni Eve potrebbe fare se fosse in grado di modificare i dati che vengono scambiati. In moltissime situazioni, modificare dati è un attacco devastante, e crea un danno molto maggiore che non semplicemente leggerli.

Ecco un altro esempio: una Storage Area Network su IP all'interno di una rete locale aziendale. Fare intercettazioni sul traffico è cosa passiva, e non svela necessariamente dati privati (in particolare su una rete basata su switch). Ma la mancanza di autenticazione permette la manomissione di dati a livello di settore, che non sarebbe possibile se ogni server avesse risorse di archiviazione proprie e non condivisibili. Aggiungere l'autenticazione evita interamente il presentarsi del problema.

Oppure, prendiamo in considerazione i nostri computer. Siccome i dati non vengono autenticati, si corre molto di più il rischio di essere vittime di virus, trojan e software maligno. Il criptaggio dei dati è importante; l'autenticazione lo è ancora di più. Se il nostro computer viene controllato da qualcun altro grazie ad un trojan, non ha molta importanza quale tipo di crittografia si è deciso di implementare.

Naturalmente ogni sistema sicuro dovrebbe avere sia crittografia che autenticazione, ma ai meno esperti l'autenticazione per pacchetto sembra soltanto un peso fastidioso e superfluo. Continuo a vedere nuovi protocolli progettati da commissioni intelligenti, che però obbligano al solo criptaggio e non all'autenticazione: WEP, Bluetooth, ecc. Una prima versione dello standard IPsec aveva una modalità per codificare ma non per autenticare.

L'anno scorso ho avuto una conversazione con un ingegnere che si occupava della sicurezza del protocollo wireless Bluetooth. Gli dissi che Bluetooth possiede solo autenticazione per la privacy e non per pacchetto. Mi rispose con le classiche scuse: 1) il salto di frequenze pseudocasuale rende "quasi impossibile" la penetrazione di un aggressore, e 2) il raggio di azione è di solo 8 piedi, per cui gli attacchi sono per forza limitati.

Ho cercato di discutere, ma alla fine ci ho rinunciato. Poi ho detto qualcosa del tipo: "Non vedo l'ora che Bluetooth diventi universale, perché mi piacerebbe davvero avere una tastiera e un mouse senza fili, con la 'base station' incorporata nel mio computer". E lui ha risposto: "Sì, ma forse Bluetooth non sarebbe adatto allo scopo, perché a quel punto qualcuno potrebbe inserire combinazioni di tasti e di clic del mouse nel tuo sistema". Non sapevo se ridere o piangere. Per la serie: esser duri di comprendonio...

** *** *****

Commenti dei lettori

Da: Ira Winkler <ira_winkler@hp.com>
Oggetto: Il contrattacco

Mi preoccupano i commenti di Jennifer Granick in risposta al tema del contrattacco. Anzitutto, il contrattacco come abitudine e condotta è cosa negativa; tuttavia ci dovrebbero essere certe condizioni in cui sia permesso intraprendere un'azione, come nel caso della gestione, da parte del DoD, di una protesta pianificata e dei bombardamenti derivanti da attacchi conosciuti come Code Red.

Tuttavia [Jennifer] ha proseguito commentando in merito alla legalità dello spam. Le sue analogie pro-spam sono una preoccupazione maggiore e una errata esposizione del problema. Nello specifico, [Jennifer] sostiene che lo spam dovrebbe essere trattato come il rumore. Lei afferma che il rumore viaggia attraverso aria o "etere", e che il rumore che viaggia fuori dai confini debba essere meglio classificato come turbativa. Ammettiamo che questo sia in qualche modo corretto. L'analogia fra spam e rumore non è nei termini di qualcuno che fa suonare il proprio stereo ad un volume così alto da essere sentito da un vicino all'interno della propria proprietà. Lo spam è invece l'equivalente di un vicino che mette lo stereo a tutto volume in modo che chiunque, in qualsiasi parte del mondo, possa sentirlo. Inoltre, la persona che fa suonare lo stereo a tutto volume ha un interesse personale nel farlo, un interesse solitamente economico. Non è dunque una turbativa involontaria, ma un infliggere intenzionalmente una seccatura per ragioni puramente egoistiche. Mi si perdoni per non essere un avvocato e non sapere le definizioni legali delle cose. È inconcepibile che un qualsiasi tribunale possa classificare questo comportamento come "turbativa generica". In aggiunta a ciò, i vari governi hanno ordinanze in merito al disturbo che classificano globalmente alcuni tipi di disturbo come inaccettabili. Lo spam è molto più assimilabile al telemarketing, che viene ora regolato da appropriate politiche di opt-out universale (la facoltà di abbandonare la lista di diffusione, ndt).

Lo spam, però, non è come il rumore. Se l'ascoltare la musica di un vicino non costa denaro a nessuno, la proliferazione dello spam costa alle aziende -- e inevitabilmente al grande pubblico -- decine di milioni di dollari. Gli ultimi studi più affidabili indicano che lo spam rappresenta oggi il 40% delle e-mail. Lo spazio per un account e-mail costa. Le transazioni via e-mail costano banda, che deve essere aumentata in relazione al traffico, compreso il traffico di spam. Le transazioni via e-mail costano in termini di utilizzo del processore, che deve essere aggiornato per sostenere un volume di traffico maggiore. I filtri anti-spam e il loro mantenimento costa denaro. Filtrare lo spam costa in termini di bassa produttività per le compagnie e per gli utenti domestici. Questi utenti sono costretti a cancellare vari account perché lo spam finisce con il far sprecare molto tempo prezioso, con la seccatura aggiuntiva di dover informare gli altri del cambio di indirizzo e-mail.

Poi vi sono le problematiche legate alla pornografia. Studi ben documentati indicano che più del 25% dello spam proviene da siti pornografici. Dato che gli spammer non tengono traccia di chi sia adulto o minore, anche i bambini finiscono col ricevere spam pornografico. La cosa peggiore è che gli spammer fanno di tutto per evitare i filtri anti-spam e anti-porno. Anche a voler usare analogie con il rumore, le pubbliche profanità e oscenità sono illegali.

Allo spam pornografico è legata una problematica a livello aziendale. Non è da escludere, per esempio, che un impiegato scontento possa -- una volta ricevuto dello spam pornografico -- denunciare il proprio datore di lavoro accusandolo di aver creato un luogo di lavoro impraticabile non applicando i dovuti filtri anti-spam.

Ad ogni modo, la parte più preoccupante dei commenti di Jennifer è quella relativa alla sua opinione secondo cui Internet è un "bene pubblico" e che quindi non ci dovrebbe essere implicazione di possesso dei computer in Internet, come per esempio i server di posta. Dio ci assista se un qualsiasi tribunale dovesse sostenere tali argomenti. Questo equivarrebbe a dire che se un computer è connesso ad Internet in qualche modo, chiunque lo può usare per farci ciò che vuole. Secondo Jennifer il computer diventa proprietà pubblica. Chiunque ha il diritto di usare il computer e i dati in esso a proprio piacimento. Seguendo questa logica, e ampliandola, si potrebbe dire che se si ha un computer connesso ad Internet in qualche modo, sarebbe illegale limitare l'accesso a quel computer. Jennifer si lamenta del fatto per cui connettersi a Internet non obbliga nessuno a rinunciare ai propri diritti di possesso su quei computer, allo stesso modo per cui guidare la propria auto lungo una strada pubblica non significa rinunciare ai diritti di proprietà sull'auto stessa.

Jennifer sostiene che proteggere i diritti di possesso sui computer connessi ad Internet è "dannoso per degli usi socialmente benefici". Estendere questo discorso al mondo reale non funziona, e non ha molto senso nemmeno per quanto riguarda Internet.

Da: Jennifer S. Granick <jennifer@granick.com>
Oggetto: Il contrattacco

Ira ed io siamo d'accordo che il contrattacco in quanto abitudine e condotta sia indesiderabile. Siamo d'accordo anche sul fatto che dovrebbero esserci alcune condizioni per cui il contrattacco sia legalmente permesso, allo stesso modo per cui non si tollera il prendere a pugni qualcuno, ma a volte lo si permette nell'ambito della difesa personale. Che cosa sia un pugno e che cosa sia legittima difesa è questione più delicata, una questione sulla quale gli avvocati hanno speso decenni nel trovarvi risposte e nel perfezionarla. Per venire al punto, io non sono d'accordo con quanto Ira implica, cioè che l'autodifesa sia un privilegio che può essere solo appannaggio del governo.

Per quanto riguarda la questione Intel contro Hamidi, chiamare spam i vari messaggi mette in ombra le reali problematiche. Ira è evidentemente molto preoccupato per quanto riguarda lo spam, la pornografia e il linguaggio osceno; più preoccupato, forse, della legge stessa, la quale afferma che tutte queste cose sono protette, in gradi differenti, dal Primo Emendamento. Piuttosto, la questione è se e quando il proprietario di un computer connesso ad Internet possa controllare quali messaggi spedisco, quali pagine web metto a disposizione e quali file trasmetto.

Ritengo che Intel abbia tutto il diritto di accordarsi con i propri impiegati per quanto concerne l'uso dei loro computer sul luogo di lavoro e di far rispettare questo accordo nei confronti degli impiegati stessi. Intel non dovrebbe avere alcun diritto di dire a me, un individuo del pubblico, quali indirizzi e-mail posso scrivere nel mio programma di posta Eudora. Intel ha poi il diritto di proteggere i propri sistemi, di richiedermi un indennizzo nel caso in cui io danneggi i loro sistemi intenzionalmente o per negligenza. Intel può cercare di filtrare i messaggi in uscita (una pratica che approvarei maggiormente se prevedesse una notifica agli utenti di ciò che sta accadendo, specialmente se si parla di provider Internet e non di compagnie private). Credo inoltre che io, in quanto utente individuale, debba poter essere in grado di dissociarmi dal ricevere messaggi commerciali non richiesti.

Tuttavia, la regola che Intel sta cercando nel caso Hamidi è quella per cui il proprietario di certi server possa ottenere ingiunzioni che impediscano ad individui del pubblico di inviare pacchetti attraverso quei server, a discrezione del proprietario, e a prescindere da ciò che l'utente finale potrebbe volere. Questa regola si applicherebbe a molte più persone che non soltanto impiegati e a molte più cose che non soltanto spam. Siccome stiamo davvero parlando di pacchetti, questa stessa regola potrebbe essere usata per obbligare Hamidi a mettere un filtro sulla sua pagina web in modo che nessun impiegato Intel possa vederla. Non credo che il mio provider Internet dovrebbe poter prendere tale decisione al mio posto.

Ira assume che un certo tipo di diritto di proprietà si possa applicare ai computer connessi in Internet, il diritto assoluto di esclusione. Perché presumere questo? Questo diritto si applica nel mondo reale soltanto alla proprietà vera e propria (la terra). La proprietà privata tradizionalmente non comprende un diritto assoluto di esclusione (questo è il dibattito sulla definizione di abuso di beni che occupa i verbali principali del caso in questione). Finché l'utente non priva il proprietario dell'uso della proprietà privata, come ad esempio rubandogli l'auto, e non ne danneggia la proprietà, il diritto del proprietario sulla proprietà non è sufficientemente infranto perché la legge possa intervenire. Posso accarezzare il tuo cane, anche se non vuoi che lo faccia.

Una regola di turbativa permette alla corte di bilanciare gli interessi del proprietario dei server, gli interessi di chi parla (il mittente) e gli interessi del pubblico nel ricevere informazioni prima di emettere un divieto. Un discorso commerciale può avere meno valore di un discorso politico. Un'ondata di e-mail irrilevanti può essere meno protetta di una serie di e-mail indirizzate ad un'utenza appropriata. Il desiderio, da parte dell'utente, di leggere ciò che il mittente ha da

dire è un elemento. I proprietari dei server sono protetti, ma lo sono anche i mittenti e gli utenti destinatari. La regola di Intel, e quella sostenuta da Winkler, va certamente bene alle aziende. Il pubblico può spedire soltanto messaggi approvati, e gli utenti possono ricevere solo messaggi approvati, e le compagnie, che siano Intel o Earthlink decidono che cosa vada approvato. AOL si rifiuta di trasmettere pacchetti provenienti da MSN Messenger. Earthlink intenta cause legali per impedire ai suoi concorrenti di inviare pubblicità di servizi meno costosi ai suoi clienti. Buon per loro, ma non è un mondo in cui voglio vivere. Né la legge impone che le cose vengano fatte in questo modo.

Si veda questo articolo, che rende maggiore giustizia a questo discorso: Dan Burk, "The Trouble with Trespass" (2000) 4 J. Small & Emerging Bus. L. 27, 49, disponibile al seguente indirizzo: <<http://www.law.umn.edu/FacultyProfiles/BurkD.htm>>.

Da: Ira Winkler <ira_winkler@hp.com>
Oggetto: Il contrattacco

Non sostengo affatto che l'autodifesa sia appannaggio del solo governo. Ho solo mostrato due esempi di autodifesa accettabile, a mio avviso, che erano i più noti. Se l'esempio del DoD riguarda il governo, l'autodifesa contro Code Red è stata attuata da entità commerciali e governative.

Per riassumere in primo luogo il caso Intel contro Hamidi, bisogna dire che Hamidi era un impiegato Intel che è stato licenziato e che ha citato Intel in giudizio. La corte si è schierata dalla parte di Intel e Hamidi, invece di andare avanti con la propria vita, ha deciso di diventare una spina nel fianco di Intel. Per molti anni, a seguito di quell'episodio, Hamidi ha fatto parecchie cose, fra cui spedire e-mail non richieste a 29.000 impiegati Intel. Come conseguenza di ciò, Intel ha cercato un'ingiunzione contro Hamidi per impedirgli di inviare nuovamente messaggi collettivi non richiesti agli impiegati Intel.

Il comportamento di Hamidi sembra ossessivo. Come facevo notare in precedenza, lo spam costa ai singoli e alle aziende milioni di dollari. Intel non è un provider Internet che offre ai propri impiegati una distribuzione di e-mail garantita. Da parte mia, ammetto di pensare che sia troppo civile chiamare "la feccia della società" tutti quelli che inviano e-mail non richieste.

Per quanto riguarda il fatto che un messaggio e-mail non richiesto sia libertà di parola, protetta dal Primo Emendamento, la posizione di Jennifer dà ad intendere che un qualsiasi individuo scelto dal mittente debba utilizzare le proprie risorse a discrezione di chiunque decida di inviargli spam su un suo account. Non sono d'accordo. Un messaggio e-mail non è solo un inoltro di pacchetti come Jennifer sostiene, ma richiede al destinatario l'uso delle risorse del proprio computer.

Il discorso secondo cui impedire a qualcuno di fare spamming voglia dire costringerlo a limitare il proprio sito web non è un'argomentazione valida e rasenta il ridicolo. Intel potrebbe decidere di bloccare il sito web a livello dei propri router, ma non può dire a nessun altro che cosa fare.

È poi discutibile l'argomentazione di Jennifer secondo cui non esistono in realtà diritti di possesso veri e propri, sia nel mondo reale che in quello virtuale. Secondo il suo discorso, per condannare qualcuno per il furto di qualsiasi cosa, occorre provare che questo qualcuno non abbia intenzione di restituirlo e che contemporaneamente si aveva l'intenzione di utilizzare l'oggetto rubato. Immaginiamo di uscire e notare che la nostra automobile non c'è più. Ad ogni modo, anche dando per buona questa argomentazione, lo spam costa in termini di archiviazione, calcolo, larghezza di banda ed elettricità, tutte cose che costano denaro. Come ho già detto, Dio ci assista se le persone non possono più avere voce in capitolo sull'uso dei computer che possiedono e mantengono una volta che questi siano connessi ad Internet.

Non vi è nulla nel caso o nelle dichiarazioni di Intel, che lascia intendere che Intel abbia l'intenzione di limitare l'e-mail o altri servizi Internet soltanto a personale autorizzato. Intel vuole solo fermare qualcuno che ha precedentemente spedito ai suoi impiegati e-mail non richieste, e dichiara che continuerà a farlo. Hamidi può usare le proprie risorse e raccogliere richieste di adesione da impiegati Intel presso i loro account di posta domestici; ad ogni modo lui e voi sapete che, con ogni probabilità, gli impiegati sono stanchi delle sue lamentele, altrimenti avrebbero già dato la loro adesione. Ancora, nulla gli sta impedendo di utilizzare le proprie risorse per far valere i propri diritti del Primo Emendamento, a parte naturalmente il fatto che a pochi interessano le sue opinioni.

Da: Jennifer S. Granick <jennifer@granick.com>
Oggetto: Il contrattacco

<< È poi discutibile l'argomentazione di Jennifer secondo cui non esistono in realtà diritti di possesso veri e propri, sia nel mondo reale che in quello virtuale. Secondo il suo discorso, per condannare qualcuno per il furto di qualsiasi cosa, occorre provare che questo qualcuno non abbia intenzione di restituirlo e che contemporaneamente si aveva l'intenzione di utilizzare l'oggetto rubato. >>

In effetti, secondo la legge comune inglese, per centinaia di anni, le cose stavano proprio così. Il furto era l'impossessarsi della proprietà altrui con _l'intento di privare permanentemente_. Se io avevo intenzione di restituirla, non si trattava di furto. In molti stati questo è stato cambiato per statuto, soprattutto per quanto concerne reati come il furto d'auto a scopo ludico. Ciò che si ritiene "proprietà" non è un diritto unico, naturale, logico e indivisibile, ma un insieme o sottoinsieme di tutti i diritti possibili che gli esseri umani hanno intenzionalmente stabilito nel tempo in modo da essere associati ai diversi tipi di proprietà, a generale vantaggio della società.

Da: Mike Robinson <miker@sundialservices.com>
Oggetto: Il contrattacco

Specialmente per quanto riguarda le problematiche legate a Internet, occorre dare uno sguardo attento ad entrambe le facce della medaglia e considerare come (e non se) una legge o principio che parta con le migliori intenzioni possa essere ritorto contro chi l'ha realizzato, nell'ambito del cyberspazio.

Per esempio, se il principio del "contrattacco" viene permesso dalla legge, allora "io in qualità di black hat" posso attaccare il tuo sistema e poi affermare, in mia difesa, che eri tu ad attaccare me e che io mi stavo semplicemente difendendo. Per corroborare la mia dichiarazione posso creare tutti i file che mi servono. Dato che la tua macchina è stata distrutta dal mio attacco, tu non hai elementi per negare le mie accuse e "la legge è dalla mia parte". Mentre tutti questi brogli legali vanno avanti (magari ho anche convinto le autorità a sequestrare le tue apparecchiature), tu ti ritrovi a terra, con la tua attività in fallimento.

Ecco perché le leggi sono scritte come sono scritte, e perché ritengo che, almeno per ora, non si può fare di meglio. Leggi ideate con le migliori intenzioni, che "legalizzano il linciaggio", vestiranno molti pali del telefono con le vestigia delle vittime... uccise, appunto, dalla legge stessa.

Da: Dorothy Denning <dedennin@nps.navy.mil>
Oggetto: Disattivare Internet

Un altro motivo per cui un governo può non voler disattivare le connessioni Internet di un avversario è il lancio di una campagna di PSYOPS (PSYchological OPERations, operazioni legate a un'azione di stampo psicologico piuttosto che militare, ndt).

Si veda: <<http://www.fcw.com/fcw/articles/2003/0113/web-iraq-01-16-03.asp>>.

Il Dipartimento della Difesa degli USA ha inviato messaggi e-mail ad ufficiali iracheni.

Da: ketil@ii.uib.no (Ketil Z. Malde)
Oggetto: Disattivare Internet

C'è un'altra ragione per cui un paese possa voler disattivare le connessioni Internet di un nemico. Le guerre riguardano sempre meno le armi in se stesse, e sempre più le informazioni, e di certo si vuole evitare che il nemico distribuisca liberamente delle informazioni alla propria opinione pubblica (si pensi a immagini vivide e colorate di bambini uccisi e mutilati -- un'inevitabile conseguenza di ogni guerra). Si osservi come una cosa del genere abbia funzionato con la guerra del Vietnam.

Questo è particolarmente importante per gli USA e i loro alleati, che sono meglio equipaggiati e preparati del nemico, e che possono combattere senza temere grosse perdite. Le persone vengono tenute lontane dal campo di battaglia, e questo le tranquillizza. Ma Internet permette a qualsiasi geek con una webcam di portare il campo di battaglia molto più vicino, senza alcuna censura militare (o rispetto della valutazione di chi osserva, che forse è ancora più efficace).

Da: Arturo Bejar <arturo@yahoo-inc.com>
Oggetto: Yahoo nel canile

Siamo stati messi nel canile! Ahimè, le informazioni riportate non sono accurate. Se un utente ha bisogno di recuperare l'accesso al proprio account, il suo compleanno è solo una delle tante informazioni che richiediamo. Anzitutto facciamo richiesta del giorno di nascita, del codice postale e dello user ID o di un secondo indirizzo e-mail. Se questi dati sono inseriti correttamente, autenticiamo l'account formulando una domanda segreta che l'utente aveva indicato all'atto della registrazione.

Se l'utente non si ricorda la risposta alla domanda segreta, agevoliamo il recupero dell'account mediante l'uso di un indirizzo e-mail alternativo verificato (è possibile verificarlo soltanto provando la conoscenza della password), una volta che sono state fornite le informazioni identificative iniziali (giorno di nascita, codice postale, user ID/secondo indirizzo e-mail).

Il messaggio di benvenuto con il proprio compleanno viene emesso solo dopo un login (ciò presume il possesso dell'account) e solo quel giorno dell'anno (data controllata dal lato server).

Se ha notizie riguardanti Yahoo! che possono essere motivo di preoccupazione, può fare riferimento a me oppure a security@yahoo-inc.com. Trattiamo con la massima serietà tutto quanto riguarda la privacy e la sicurezza degli utenti e cerchiamo di rispondere prontamente ad ogni problematica che viene sollevata.

** **

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 Sec