

CRYPTO-GRAM  
15 luglio 2008

Scritta da Bruce Schneier  
Fondatore e CTO di BT Counterpane

Edizione italiana curata da Communication Valley SpA  
<<http://www.communicationvalley.it/>>

CRYPTO-GRAM è una newsletter mensile gratuita che offre riassunti, analisi, approfondimenti, e commenti sulla sicurezza (informatica e in generale) e sulla crittografia.

Per consultare i numeri arretrati, o per iscriversi, andare all'indirizzo:  
<<http://www.schneier.com/crypto-gram.html>>.

Oppure si può leggere il presente numero direttamente sul Web, all'indirizzo:  
<<http://www.schneier.com/crypto-gram-0703.html>>.

Gli stessi articoli della newsletter sono disponibili sul blog di Bruce Schneier "Schneier on Security": <<http://www.schneier.com/blog>>.

Crypto-Gram è anche consultabile in formato RSS.

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

In questo numero:

- Le telecamere a circuito chiuso
- News
- Interruttori d'emergenza e controllo remoto
- LifeLock e il furto d'identità
- Le news su Schneier/BT Counterpane
- Il primo Workshop interdisciplinare sulla Sicurezza e il comportamento umano
- La verità sugli hacker cinesi
- Attacchi man-in-the-middle
- Commenti dei lettori

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

Le telecamere a circuito chiuso

Un sistema capillare di telecamere di sicurezza non serve a ridurre l'incidenza del crimine, almeno non in maniera significativa. Esistono delle eccezioni, naturalmente, e sono queste che finiscono in mano alla stampa. Il caso più eclatante avvenne nel 1993, quando le telecamere di sicurezza contribuirono alla cattura degli assassini di James Bulger. E qualche mese fa hanno contribuito a condannare Steve Wright per l'uccisione di cinque donne nella zona di Ipswich. Ma queste sono le eccezioni maggiormente pubblicizzate. In generale, le telecamere a circuito chiuso non sono molto efficaci.

È un fatto che è stato più volte dimostrato: da uno studio approfondito del 2005 per il Ministero dell'Interno USA, da altri studi negli Stati Uniti, e ancora da nuovi dati resi noti lo scorso mese da New Scotland Yard. I criminali che aiutano a risolvere sono davvero pochi, e il loro effetto deterrente è minimo.

L'opinione prevalente si aspetterebbe il contrario. Ma se ciò fosse vero, Londra, che ha installato 500.000 telecamere di sorveglianza, sarebbe la città più sicura del pianeta. Non lo è, ovviamente, a causa dei limiti tecnologici delle telecamere, dei limiti organizzativi della polizia, e della capacità di adattarsi dei criminali.

Per alcuni è confortante immaginare solerti agenti di polizia mentre controllano ogni telecamera, ma la realtà è piuttosto diversa. Gran parte di quel che viene ripreso viene ignorato, e visionato solo molto tempo dopo che è stato commesso un reato. E quando i filmati vengono esaminati, capita di frequente che gli osservatori non riescano a identificare i sospettati. L'illuminazione è pessima e le immagini sgranate, e i criminali tendono a evitare di fissare direttamente verso la telecamera. Questi aggeggi, poi, si rompono troppo spesso. E anche i migliori sistemi di videosorveglianza possono essere ostacolati usando occhiali da sole o cappelli. Anche quando permettono una rapida identificazione di un criminale (si pensi ai dinamitardi dei trasporti pubblici a Londra nel 2005 e ai terroristi dell'11 settembre), spesso la polizia è in grado di identificare i sospettati senza l'ausilio delle telecamere. Le telecamere danno una falsa impressione di sicurezza, e invitano alla pigrizia, mentre abbiamo bisogno di un corpo di polizia vigile e attento.

Che la polizia si metta a controllare costantemente tutte le telecamere non è però una soluzione. Le telecamere a circuito chiuso, a differenza di un agente di polizia che cammina per la strada, possono soltanto osservare certi luoghi in certe direzioni. I criminali lo sanno, e si adattano facilmente commettendo reati in altri luoghi non videosorvegliati -- e luoghi del genere ci saranno sempre. Inoltre, mentre un agente di polizia per la strada può rispondere immediatamente in caso di reato, lo stesso agente di fronte a un monitor può al massimo inviare un altro agente, che arriverà comunque tardi sul luogo del crimine. A causa della loro stessa natura, l'effetto prodotto dalle telecamere a circuito chiuso è un utilizzo ridotto e male indirizzato delle risorse di polizia.

Le telecamere non sono totalmente inutili, ovvio. In alcune circostanze sono efficaci nel ridurre il crimine in aree circoscritte e con un passaggio limitato di persone a piedi. In presenza di buona illuminazione, riducono sostanzialmente sia le aggressioni che i tentativi di furto nei parcheggi. E da un certo punto di vista, spingere i criminali altrove è già un buon risultato. Se un negozio della catena Tesco installa delle telecamere al suo interno, e per questo un ladro preferisce prendere di mira il negozio a fianco, per Tesco sono soldi ben spesi. Solo che non viene ridotto il tasso di crimine generale, pertanto è uno spreco di denaro per la cittadinanza.

Ma la questione, in realtà, non è se le telecamere riducano o meno il crimine; la questione è se valgono davvero la pena. E considerandone il costo (500 milioni di sterline negli ultimi dieci anni), la loro limitata efficacia, il potenziale abuso (spiare donne nude nelle proprie case, passarsi immagini di nudo, vendere i video con le "scelte migliori", e persino spiare uomini politici) e i loro effetti orwelliani sulla privacy e sulle libertà civili, molto spesso no, non valgono la pena. Il denaro investito in sistemi di sorveglianza a circuito chiuso sarebbe molto meglio spenderlo assumendo agenti di polizia esperti.

Stiamo vivendo un periodo unico nella nostra società: le telecamere sono dappertutto, e possiamo ancora vederle. Dieci anni fa, la loro presenza era molto meno massiccia. E fra dieci anni saranno talmente piccole che non le noteremo nemmeno. Vi sono già aziende come L-1 Security Solutions che stanno sviluppando per la Cina tecnologie di videosorveglianza da stato di polizia, come il riconoscimento facciale; tecnologie che troveranno il modo di approdare in paesi come il Regno Unito. È necessario stabilire dei limiti a questa tecnologia prima che le telecamere diventino così piccole da non essere più notate.

Ricerche sulle telecamere a circuito chiuso:

<<http://electronics.howstuffworks.com/police-camera-crime1.htm>>  
<<http://www.scotcrim.u-net.com/researchc2.htm>>  
<<http://news.bbc.co.uk/1/hi/uk/2192911.stm>>  
<<http://www.homeoffice.gov.uk/rds/pdfs05/hors292.pdf>>  
<<http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2007/08/14/MNIPRHRPE.DTL>>  
oppure <<http://tinyurl.com/688f76>>  
<<http://www.temple.edu/cj/misc/PhilaCCTV.pdf>>  
<<http://archives.cnn.com/2002/LAW/10/21/ctv.cameras/>>  
<<http://www.guardian.co.uk/uk/2008/may/06/ukcrime1>>

Le telecamere di Londra:

<<http://www.channel4.com/news/articles/society/factcheck+how+many+cctv+cameras/2291167>>  
oppure <<http://tinyurl.com/65vwq8>>  
<[http://www.ico.gov.uk/upload/documents/library/data\\_protection/practical\\_application/surveillance\\_society\\_full\\_report\\_2006.pdf](http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf)>  
oppure <<http://tinyurl.com/ya76db>>

Videosorveglianza e abusi:

<[http://news.bbc.co.uk/2/hi/uk\\_news/england/merseyside/4609746.stm](http://news.bbc.co.uk/2/hi/uk_news/england/merseyside/4609746.stm)>  
<<http://www.timesonline.co.uk/tol/news/uk/article743391.ece>>  
<<http://news.bbc.co.uk/2/hi/europe/4849806.stm>>

Telecamere 'orwelliane':

<<http://wuntvor.mirror.waffleimages.com/files/44/44cb4b91287cfd8111d471867502a3cac861ab0.jpg>>  
oppure <<http://tinyurl.com/3l8jtk>>  
<<http://lifeandhealth.guardian.co.uk/family/story/0,,2280044,00.html>>

Preoccupazioni per la privacy:

<<http://epic.org/privacy/surveillance/>>  
<<http://www.aclu.org/privacy/spying/14863res20020225.html>>

Sorveglianza in Cina:

<[http://www.rollingstone.com/politics/story/20797485/chinas\\_allseeing\\_eye](http://www.rollingstone.com/politics/story/20797485/chinas_allseeing_eye)>  
oppure <<http://tinyurl.com/5zwc5w>>

Una confutazione:

<<http://www.guardian.co.uk/commentisfree/2008/jul/03/ukcrime.civilliberties>>  
oppure <<http://tinyurl.com/66ryhp>>

Commenti:

<<http://gritsforbreakfast.blogspot.com/2008/07/schneier-nows-time-to-limit-cctv-waste.html>>

oppure <<http://tinyurl.com/6jsexf>>

Altri ottimi articoli:

<<http://ipvideomarket.info/review/show/145>>

<<http://gritsforbreakfast.blogspot.com/2008/07/cctv-proponents-should-abandon-claims.html>>

oppure <<http://tinyurl.com/5erp65>>

Questo articolo è stato originariamente pubblicato sul Guardian.

<<http://www.guardian.co.uk/technology/2008/jun/26/politics.ukcrime>>

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

News

Il worm Storm viene utilizzato per vendere farmaci come il Viagra.

<[http://www.darkreading.com/document.asp?doc\\_id=156139&WT.svl=news1\\_1](http://www.darkreading.com/document.asp?doc_id=156139&WT.svl=news1_1)>

<[http://www.schneier.com/blog/archives/2007/10/the\\_storm\\_worm.html](http://www.schneier.com/blog/archives/2007/10/the_storm_worm.html)>

Non ho mai capito che cos'abbia di speciale il cosiddetto ransomware. Sì, cripta i vostri dati e vi viene chiesto del denaro se volete la chiave per decrittarli. Ma non è peggiore dei vecchi virus che visualizzavano un messaggio spiritoso sullo schermo e vi cancellavano il disco rigido. La cosa più importante che un'azienda o un individuo possano fare per migliorare la sicurezza è avere un'ottima strategia di backup. È stato così per anni, ed è ancora valido oggi.

<[http://blogs.computerworld.com/ransomware\\_malware\\_armageddon\\_approaches](http://blogs.computerworld.com/ransomware_malware_armageddon_approaches)>

oppure <<http://tinyurl.com/6bf7lm>>

Attacco alle serrature elettroniche grazie a un anello magnetico: impressionante.

<<http://www.toool.nl/blackbag/?p=204>>

Un'eccellente storia di "sicurezza per segretezza", su una collezione di monete e valuta del valore di centinaia di milioni di dollari che è stata spostata senza troppe misure di sicurezza:

<[http://www.schneier.com/blog/archives/2008/06/security\\_throug\\_1.html](http://www.schneier.com/blog/archives/2008/06/security_throug_1.html)>

È possibile intercettare dati vocali compressi e criptati, almeno in minima parte, mediante l'analisi del traffico:

<<http://technology.newscientist.com/channel/tech/dn14124-compressed-web-phone-calls-are-easy-to-bug.html>>

oppure <<http://tinyurl.com/3u7j6b>>

Una macchina per il caffè Jura F90 può essere hackerata remotamente via Internet.

<<http://www.securityfocus.com/archive/1/493387>>

Una delle soluzioni finaliste nel concorso Underhanded C Contest dello scorso anno era un'implementazione scorretta di RC4 che, dopo un certo periodo di utilizzo, passava

semplicemente il testo in chiaro, senza crittografia. Plausibilmente negabile, e assai brillante.

<[http://underhanded.xcott.com/?page\\_id=9](http://underhanded.xcott.com/?page_id=9)>

Dilbert e la sorveglianza sul posto di lavoro:

<<http://dilbert.com/strips/comic/2008-06-20/>>

Una nuova tecnologia per rilevare agenti chimici, biologici ed esplosivi.

[https://publicaffairs.llnl.gov/news/news\\_releases/2007/NR-07-03-07.html](https://publicaffairs.llnl.gov/news/news_releases/2007/NR-07-03-07.html)

oppure <<http://tinyurl.com/54rmk4>>

Delle piscine intorno a Shanghai stanno esaminando i liquidi odorandoli. Questo divieto sui liquidi sta assumendo forme sempre più bizzarre.

<<http://www.reuters.com/article/oddlyEnoughNews/idUSPEK18633820080620>>

Un nuovo studio sostiene che gli insider (coloro che lavorano all'interno di un'azienda o struttura) non sono la minaccia principale per la sicurezza di rete. Tutto il dibattito 'insider contro outsider' è sempre stato più che altro una questione di semantica. Se ci si limita a contare gli attacchi, è chiaro che vi sarà un maggior numero di attacchi dall'esterno. Se si contano gli incidenti, i numeri tendono ad avvicinarsi: 75% contro il 18% in questo caso. E se si tengono in considerazione i danni provocati da un attacco a buon fine, in genere il primato spetta agli insider, specialmente perché possiedono molte più informazioni dettagliate e possono orchestrare meglio i propri attacchi. Le minacce, interne ed esterne, sono entrambe un rischio per la sicurezza, ed è necessario difendersi da entrambe. Cercare di stilare classifiche non mi pare sia tanto utile.

<[http://www.pcworld.com/businesscenter/article/147098/insider\\_threat\\_exaggerated\\_study\\_says\\_.html](http://www.pcworld.com/businesscenter/article/147098/insider_threat_exaggerated_study_says_.html)>

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

Il sindaco di Toronto, David Miller, rivela un modo un po' confuso di ragionare sulla sicurezza: "In un'epoca in cui non è possibile portare in aereo un grosso tubetto di dentifricio, com'è possibile permettere l'introduzione di pistole nella Union Station, il principale snodo di transito canadese?", ha domandato ai suoi colleghi del consiglio comunale". Secondo questo ragionamento, credo si possa proibire qualunque cosa in qualunque luogo.

<[http://toronto.ctv.ca/servlet/an/local/CTVNews/20080623/gun\\_violence\\_080623/20080623/?hub=TorontoNewHome](http://toronto.ctv.ca/servlet/an/local/CTVNews/20080623/gun_violence_080623/20080623/?hub=TorontoNewHome)>

oppure <<http://tinyurl.com/6dqbc0>>

Gli adolescenti inglesi si servono di Google Earth per trovare piscine in cui organizzare crash party. Quanto passerà prima che qualcuno trovi un reato molto più serio da commettere grazie all'ausilio di Google Earth?

<[http://www.reghardware.co.uk/2008/06/18/tech\\_aids\\_pool\\_crashing/](http://www.reghardware.co.uk/2008/06/18/tech_aids_pool_crashing/)>

Ho visto le pistole a infrarossi per effettuare lo screening in diversi aeroporti, soprattutto in Asia. L'idea è quella di allontanare persone con l'influenza aviaria, o con qualsiasi altra 'malattia-spauracchio'. Questo articolo spiega perché non funzionano:

<[http://scienceblogs.com/effectmeasure/2008/06/why\\_fever\\_screening\\_at\\_airport.php](http://scienceblogs.com/effectmeasure/2008/06/why_fever_screening_at_airport.php)>

oppure <<http://tinyurl.com/69tht2>>

Piccioni viaggiatori usati per portare merci di contrabbando nelle prigioni in Brasile:

<<http://news.bbc.co.uk/1/hi/world/americas/7472537.stm>>

Credo che questa sia la prima vulnerabilità di sicurezza trovata nella RFC 1149: "Standard per la trasmissione di datagrammi IP su corrieri aviari". L'ispezione deep packet sembra essere l'unico sistema per prevenire tale attacco, anche se un adeguato contenimento impedirà addirittura l'avvio del protocollo.

<<http://www.faqs.org/rfcs/rfc1149.html>>

Una 'top ten' dei brevetti antiterrorismo; no, non è uno scherzo. Il mio preferito è la botola per aeroplani.

<<http://www.neatorama.com/2008/06/27/top-10-strangest-anti-terrorism-patents/>>  
oppure <<http://tinyurl.com/5sct5d>>

Il Pentagono si sta avvalendo della consulenza di scienziati sociali in merito alle questioni di sicurezza. L'articolo parla molto dei potenziali conflitti di interesse e cose del genere, e meno di quali siano i contributi che gli scienziati sociali possano offrire. Penso vi sia molto potenziale a tale proposito.

<<http://www.nytimes.com/2008/06/18/arts/18minerva.html>>

Uno degli autori, forse l'unico autore, del worm Nugache è stato arrestato nel Wyoming. Il diciannovenne si dichiarerà colpevole.

<<http://blog.wired.com/27bstroke6/2008/06/hacker-launches.html>>

<<http://www.jacksonholestartrib.com/articles/2008/06/30/news/wyoming/doc48656c8a93378754215938.txt>>

oppure <<http://tinyurl.com/4obdmo>>

È da un po' di tempo che non parlo delle macchine per il voto elettronico, ma Dan Wallach ha scritto un post eccellente sul suo blog in merito all'attuale linea di pensiero delle aziende produttrici di tali macchine, e perché è sbagliata.

<<http://www.freedom-to-tinker.com/?p=1304>>

Questo studio misura l'insicurezza nell'insieme globale dei browser, sfruttando i log dei server Web di Google. Perché tutto ciò è importante? Perché i browser sono un vettore di attacco sempre più diffuso. I risultati non sono buoni.

<<http://www.techzoom.net/publications/insecurity-iceberg/index.en>>

<<http://www.ofcourseimright.com/?p=29>>

Stupidaggini in nome del terrorismo, prima parte: in Canada, un impiegato di una linea aerea prima dice a una viaggiatrice che è "illegale" pronunciare certe parole, poi la avverte che se causerà problemi verrà falsamente accusata.

<<http://www.theglobeandmail.com/servlet/story/RTGAM.20080627.blatch28/BNStory/specialComment/home>>

oppure <<http://tinyurl.com/6b927p>>

Stupidaggini in nome del terrorismo, seconda parte: un cittadino britannico è costretto ad abbandonare il proprio hobby -- fotografare autobus -- perché viene infastidito e ostacolato sempre più spesso.

<[http://www.theregister.co.uk/2008/06/24/bus\\_spotter\\_clampdown/](http://www.theregister.co.uk/2008/06/24/bus_spotter_clampdown/)>

Stupidaggini in nome del terrorismo, terza parte: gli israeliani chiamano 'terrorista' un pazzo omicida palestinese:

<<http://www.cnn.com/2008/WORLD/meast/07/02/israel.bulldozer/>>

Stupidaggini in nome del terrorismo, quarta parte: una scuola pubblica del New Jersey viene chiusa dopo che qualcuno ha visto un Ninja. Risulta che il Ninja era in realtà un capogruppo del campeggio per ragazzi in tenuta nera da karate e con una spada di plastica.

<[http://www.boston.com/news/odd/articles/2008/06/25/school\\_locked\\_down\\_after\\_ninja\\_sighted\\_in\\_woods/](http://www.boston.com/news/odd/articles/2008/06/25/school_locked_down_after_ninja_sighted_in_woods/)>

oppure <<http://tinyurl.com/6h84n2>>

Ottima prima pagina per un quotidiano: "Una giraffa aiuta cammelli e zebre a scappare da un circo".

<<http://ap.google.com/article/ALeqM5h1AqbvSMYPxJrla6-Fgym8WIZesgD91KNJD00>>

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

Il Regno Unito sta imparando che criptare i dischi significa che non ci si deve preoccupare in caso di smarrimento.

<[http://www.schneier.com/blog/archives/2008/07/encrypting\\_disk.html](http://www.schneier.com/blog/archives/2008/07/encrypting_disk.html)>

Cravatte che in realtà sono bombe a orologeria. Da non indossarsi negli aeroporti.

<[http://www.etsy.com/view\\_listing.php?listing\\_id=12792904](http://www.etsy.com/view_listing.php?listing_id=12792904)>

Il profiling automatizzato non serve a niente:

<[http://www.theregister.co.uk/2008/06/24/home\\_office\\_passenger\\_profiling/](http://www.theregister.co.uk/2008/06/24/home_office_passenger_profiling/)>

oppure <<http://tinyurl.com/5p9e6n>>

Ma gli Stati Uniti vogliono implementarlo ugualmente: "Il Dipartimento di Giustizia sta considerando l'idea di permettere all'FBI di indagare sui cittadini americani senza alcuna prova che giustifichi un'indagine, affidandosi invece a un profilo di terrorista che potrebbe isolare musulmani, arabi o altri gruppi razziali o etnici".

<[http://www.usatoday.com/news/washington/2008-07-02-terror-profiling\\_N.htm](http://www.usatoday.com/news/washington/2008-07-02-terror-profiling_N.htm)>

oppure <<http://tinyurl.com/5nvt5>>

Ho già scritto in merito al profiling:

<<http://www.schneier.com/blog/archives/2005/07/profiling.html>>

Questi sono occhiali da sole che nascondono il vostro volto dalle telecamere. Non so dire se è tutto vero oppure se è una colossale burla.

<<http://www.hackaday.com/2008/06/27/anti-paparazzi-sunglasses/>>

<<http://www.abrutis.com/video-lunettes+anti+paparazzi-11937.html>>

In un progressivo inflazionamento del termine 'terrorismo', il Premier del New South Wales ha definito un potenziale sciopero dei lavoratori delle ferrovie "tattica di terrore industriale". Il terrorismo è un crimine atroce, e un grave problema internazionale. Non è una parola jolly per descrivere qualsiasi cosa non ci piaccia o che non approviamo, né qualcosa che abbia un effetto negativo per un gran numero di persone. Impiegando il termine 'terrorismo' indiscriminatamente e in maniera più libera di quanto intenda il suo reale significato, confondiamo ancor di più i concetti più diffusi della questione. La parola 'terrorismo' ha un significato ben preciso, e non dovremmo svilarlo.

<<http://www.news.com.au/story/0,23599,23981698-421,00.html>>

George Carlin sulla sicurezza aeroportuale, prima dell'11 settembre.

<<http://www.youtube.com/watch?v=KBxzvSbGJ2w>>

I ladruncoli stanno sfruttando la "guerra alla fotografia" per rubare schede di memoria:

<[http://www.schneier.com/blog/archives/2008/07/exploiting\\_the.html](http://www.schneier.com/blog/archives/2008/07/exploiting_the.html)>

Un articolo eccellente sulla stupidità della TSA:

<[http://www.schneier.com/blog/archives/2008/07/good\\_essay\\_on\\_t\\_1.html](http://www.schneier.com/blog/archives/2008/07/good_essay_on_t_1.html)>

Una vignetta sul tema del password guessing:

<[http://www.cartoonbank.com/product\\_details.asp?mcsid=QCH1RR81LSM79KXHUFA C1SUSE8V18VU3&sitetype=1&did=4&sid=125244](http://www.cartoonbank.com/product_details.asp?mcsid=QCH1RR81LSM79KXHUFA C1SUSE8V18VU3&sitetype=1&did=4&sid=125244)>

oppure <<http://tinyurl.com/59p9mc>>

Daniel Solove sulla nuova legge FISA:

<[http://www.concurringopinions.com/archives/2008/07/the\\_new\\_foreign.html](http://www.concurringopinions.com/archives/2008/07/the_new_foreign.html)>

Utilizzare uno strumento per la cancellazione dei file è considerato sospetto:

<<http://www.latimes.com/technology/la-fi-consumer6-2008jul06,0,325447.story>>

Ombrelli da combattimento indistruttibili.

<<http://blog.wired.com/gadgets/2008/07/unbreakable-fig.html>>

Non perdetevi il filmato.

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

Interruttori d'emergenza e controllo remoto

Prima era soltanto l'industria dell'intrattenimento a voler controllare i nostri computer (e televisori, e iPod, e tutto il resto) per garantire che non violassimo nessuna delle leggi sul copyright. Ma adesso un po' tutti vogliono metterci i bastoni fra le ruote.

OnStar presto consentirà alla polizia di spegnere il motore di un'auto da remoto. La stessa funzione verrà applicata agli autobus, in caso qualche terrorista voglia riproporre il film "Speed" nella vita reale. Il Pentagono vuole che siano installati interruttori di emergenza (kill switch) sugli aerei ed è preoccupato che dei potenziali nemici possano fare altrettanto.

Microsoft, in quest'ambito, ci sta mettendo il pensiero più creativo possibile, con qualcosa chiamato "Digital Manners Policies" (grosso modo 'politiche di buon comportamento digitale'). Secondo questo brevetto di applicazione, ogni dispositivo dotato di DMP accetterebbe 'ordini' trasmessi da remoto per limitare le proprie funzionalità. I telefoni cellulari potrebbero essere impostati da remoto in modalità silenziosa in ristoranti e sale da concerto, ed essere spenti sugli aerei e negli ospedali. Alle macchine fotografiche potrebbe venir impedito di scattare foto in spogliatoi e musei, e i dispositivi di registrazione potrebbero essere disattivati nei teatri. I professori potrebbero finalmente impedire agli studenti di inviarsi messaggi SMS durante le lezioni.

Le possibilità sono infinite, e molto pericolose. Far funzionare questo modello significa costituire un sistema gerarchico di autorità praticamente senza difetti. È un arduo problema di sicurezza anche nella sua forma più semplice. Distribuire tale sistema attraverso una serie di dispositivi differenti (computer, telefoni, PDA, macchine fotografiche, attrezzature di registrazione) con firmware diversi e prodotti da aziende diverse, è ancora più difficile. Senza contare il delegare livelli di autorità differenti a

varie agenzie, aziende, industrie e singoli individui, e il far rispettare le misure di salvaguardia necessarie.

Una volta imboccato questo sentiero (affidare a un dispositivo un'autorità su altri dispositivi), i problemi di sicurezza iniziano ad accumularsi. Chi ha l'autorità per limitare le funzionalità dei miei dispositivi, e come l'ha ottenuta? Che cosa impedisce a queste persone di abusare di tale potere? Mi viene data la possibilità di annullare le limitazioni da loro imposte? Come, e in quali circostanze? E loro possono annullare i miei annullamenti?

Come è possibile evitare che questo modello venga abusato? Può uno scassinatore, per esempio, far valere una regola "vietato fotografare" e impedire il funzionamento delle telecamere di sicurezza? Possono le forze dell'ordine far valere la stessa regola per evitare un altro pasticcio come quello di Rodney King? Verranno forniti alla polizia dei dispositivi da 'superutente', non soggetti a limitazioni, e dispositivi 'super-controllori' che possono imporre limitazioni a qualunque altro dispositivo? Come possiamo assicurarci che solamente la polizia riceva tali strumenti, e che faremo quando tali apparecchiature finiranno inevitabilmente nelle mani sbagliate?

È relativamente semplice far funzionare questo modello in sistemi specializzati chiusi (OnStar, l'avioelettronica dei velivoli, l'hardware militare) ma molto più complesso in sistemi aperti. Se pensate che l'idea di Microsoft possa essere progettata in maniera sicura, basti osservare la risibile efficacia dei vari sistemi anticopia e di protezione dei diritti digitali che sono stati prodotti in questi anni. È un analogo meccanismo di imposizione di funzionalità, solo più semplice di questi altri sistemi più generici.

Ed è la chiave per comprendere questo sistema. Non facciamoci ingannare dalle storie di terrore sui dispositivi wireless sugli aerei e negli ospedali, o dalle visioni di un mondo in cui nessuno più chiacchiera ad alta voce al cellulare in ristoranti di lusso. In realtà si tratta semplicemente delle aziende di multimedia che vogliono esercitare un controllo ancora maggiore sui nostri dispositivi. Non solo non vogliono che film e concerti vengano registrati di nascosto, ma anche che il nuovo televisore imponga le 'buone maniere' al computer, impedendogli di registrare i programmi. Vogliono che l'iPod si rifiuti cortesemente di copiare musica su un computer diverso dal nostro. Vogliono imporre la PROPRIA definizione legale di 'maniere': controllare quel che facciamo e quando, e farci pagare ripetutamente per i privilegi concessi appena se ne presenta l'occasione.

"Digital Manners Policies" è un termine di marketing. Chiamiamolo per quel che veramente è: Selective Device Jamming, ovvero jamming selettivo dei dispositivi. Non è corretto, ed è pericoloso. E non renderà nessuno più sicuro, o più corretto.

Gli interruttori di emergenza (kill switch):

<<http://www.informationweek.com/news/mobility/showArticle.jhtml?articleID=202400922>>

oppure <<http://tinyurl.com/6jy2ac>>

<[http://www.nypost.com/seven/06082008/news/regionalnews/busting\\_terror\\_114567.htm](http://www.nypost.com/seven/06082008/news/regionalnews/busting_terror_114567.htm)>

oppure <<http://tinyurl.com/5p5kaj>>

<<http://blog.wired.com/defense/2008/06/the-pentagons-n.html>>

<<http://spectrum.ieee.org/may08/6171>>

Digital Manners Policies:

<<http://arstechnica.com/news.ars/post/20080611-microsoft-patent-brings-miss-manners-into-the-digital-age.html>>

oppure <<http://tinyurl.com/449bcc>>

<<http://appft1.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PG01&p=1&u=%2Fnetacgi%2FPTO%2Fsrchnum.html&r=1&f=G&l=50&s1=%2220080125102%22.PGNR.&OS=DN/20080125102&RS=DN/20080125102>>

oppure <<http://tinyurl.com/68thpf>>

Questo articolo è originariamente apparso su Wired.com.

<[http://www.wired.com/politics/security/commentary/securitymatters/2008/06/securitymatters\\_0626](http://www.wired.com/politics/security/commentary/securitymatters/2008/06/securitymatters_0626)>

oppure <<http://tinyurl.com/4htrb4>>

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

LifeLock e il furto d'identità

LifeLock, una delle aziende che offrono protezione da furti d'identità negli Stati Uniti, si trova nell'occhio del ciclone ultimamente. È stata denunciata da agenzie di credito, da compagnie della concorrenza e da avvocati in vari stati che stanno intentando cause class action. Più le vicende riportate dai media... Insomma, cibo per piranha.

Vi sono anche molti errori e fraintendimenti. Con la sua campagna aggressiva e un CEO che pubblica il suo numero di Previdenza Sociale e sfida chiunque a rubare la sua identità (Todd Davis, n. 457-55-5462), LifeLock è una compagnia facile da odiare. Ma la storia di questa azienda ha da offrire qualche interessante lezione di sicurezza, e vale la pena approfondirla e comprenderla.

Nel dicembre 2003, secondo il Fair and Accurate Credit Transactions Act, o FACTA, le agenzie di credito venivano obbligate a permettervi di inserire un avviso di frode nei loro rapporti di credito, richiedendo ai prestatori di verificare la vostra identità prima di emettere una carta di credito a vostro nome. Tale avviso è temporaneo, e scade dopo 90 giorni. Spuntano molte nuove aziende -- LifeLock, Debix, LoudSiren, TrustedID -- che rinnovano automaticamente questi avvisi, rendendoli di fatto permanenti.

Tale servizio manda in bestia le agenzie di credito e i loro clienti finanziari. Il motivo per cui i prestatori non verificano periodicamente la vostra identità prima di fornirvi un credito è che si tratta di un processo lungo, che costa denaro, e che è un altro ostacolo fra voi e un'altra carta di credito. (Comprare, comprare, comprare -- è l'imperativo americano). Pertanto, agli occhi delle agenzie di credito, i clienti di LifeLock sono 'merce di qualità inferiore'; le loro informazioni non sono così preziose da vendere. Inoltre LifeLock dissocia i propri clienti dalle offerte pre-approvate delle carte di credito, rendendoli ancora meno 'preziosi' per le agenzie di credito.

E quindi iniziò una campagna diffamatoria da parte delle agenzie di credito. Potete leggere il loro punto di vista nell'articolo del New York Times, scritto da un reporter che non ha fatto altro che ripetere acriticamente le loro posizioni. E le cause class action

hanno esagerato, accusando LifeLock di pratiche commerciali ingannevoli, pubblicità fraudolenta, e così via. La calunnia più grande è stata dire che LifeLock non ha protetto nemmeno Todd Davis, e che si suppone che la sua identità sia stata rubata.

No, non è stata rubata. Qualcuno nel Texas ha utilizzato il numero di Previdenza Sociale di Davis per ottenere un anticipo di 500 dollari sulla sua busta paga. Ha funzionato perché l'operazione di prestito non ha effettuato controlli con nessuna agenzia di credito prima di approvare il prestito -- cosa assolutamente normale per una quantità di denaro così piccola. Davis è stato chiamato per presentarsi e ritirare il denaro, e LifeLock ha chiarito il problema. Il suo rapporto di credito rimane senza macchia.

La causa intentata dall'agenzia di credito Experian sostiene in pratica che gli avvisi di frode sono riservati soltanto a chi è stato vittima di un furto di identità. Ciò sembra quantomeno spurio: il testo della legge sostiene che chiunque "afferma il sospetto in buona fede che il cliente è stato o sta per essere vittima di frode o di un reato analogo" può richiedere un avviso di frode. A me sembra che includa chiunque abbia ricevuto una di quelle notifiche sullo smarrimento o furto delle proprie informazioni finanziarie, ossia tutti.

Per quanto riguarda le pratiche commerciali ingannevoli e la pubblicità fraudolenta, paiono proprio delle esagerazioni da parte dei legali che stanno portando avanti le cause class action. Il marketing di LifeLock, aggressivo e basato sulla paura, non sembra tanto peggiore di tante altre simili campagne pubblicitarie. Secondo me queste cause class action non andranno da nessuna parte.

In realtà, l'obbligare i prestatori a verificare l'identità prima di emettere un credito è esattamente quel che dovremmo fare per combattere il furto d'identità. Esistono sostanzialmente due metodi per contrastare il furto d'identità: rendere le informazioni personali più difficili da rubare, e rendere le informazioni personali rubate più difficili da riutilizzare. Sappiamo tutti che il primo metodo non funziona, e quindi rimane il secondo. Se il Congresso volesse risolvere il problema per davvero, una delle cose che farebbe sarebbe impostare gli avvisi di frode permanenti per tutti. Ma i lobbisti dell'industria del credito non lo permetterebbero mai.

LifeLock svolge una serie di attività intelligenti. Controlla il database nazionale degli indirizzi e vi avverte se il vostro indirizzo viene cambiato. Cerca i vostri numeri di carta di credito e di debito sui siti Web di hacker e criminali, e in caso li trovi vi assiste nel processo di ottenimento di un nuovo numero. Possiedono una garanzia di servizio da un milione di dollari (per complicate ragioni legali non possono chiamarla assicurazione) per aiutarvi nel caso la vostra identità venga rubata.

Ma pur con tutto questo, non sono uno dei clienti di LifeLock. Per 120 dollari l'anno non vale la pena. Considerando l'attenzione della stampa, uno non se lo aspetterebbe, ma trattare il furto d'identità è diventato più semplice e più di routine. Certo, è un problema che si sta diffondendo: secondo i dati della Federal Trade Commission, 8,3 milioni di americani sono stati vittima di furti di identità nel 2005. Ma ciò comprende anche quei casi in cui una persona vi ruba la carta di credito e la utilizza, una cosa che raramente vi costa denaro e contro la quale, fra l'altro, LifeLock non offre protezione. La frode legata a nuovi conti aperti in vostro nome è molto meno comune, e colpisce 1,8 milioni di americani all'anno, ossia lo 0,8 per cento della popolazione adulta. La FTC non ha pubblicato cifre per il 2006 e 2007, ma il tasso sembra essere in diminuzione.

Anche la frode legata all'apertura di nuove carte di credito non è particolarmente dannosa. L'ammontare medio della frode commessa dal ladro è 1.350 dollari, ma non si è responsabili per questo. Malgrado alcune storie davvero orribili di furti d'identità, l'industria finanziaria è piuttosto brava a rimediare velocemente ai pasticci. In media, il costo che incide sulla vittima di una simile frode è 40 dollari, più una decina di ore di scocciatura per risolvere il problema. Anche assumendo che il vostro tempo valga 100 dollari a ora, LifeLock non vale più di 8 dollari l'anno.

Ed è difficile ottenere dati che misurino la reale efficacia di LifeLock. L'azienda è sul mercato da tre anni e ha circa un milione di clienti, ma la maggior parte di questi lo è diventata nell'ultimo anno. Ha sborsato denaro 113 volte per la sua garanzia di servizio, ma in molti casi per incidenti avvenuti prima che i loro clienti diventassero clienti (suppongo fosse più semplice pagare che discutere). Ma in realtà non sanno quanto spesso gli avvisi di frode sorprendano in flagrante un ladro di identità. A mio avviso la frequenza è minore di quello 0,8 per cento di incidenza di frode di cui si parlava poco sopra.

Il business model di LifeLock si basa più sulla paura del furto di identità che sui rischi veri e propri.

È davvero ironico che le agenzie di credito attacchino LifeLock per le sue pratiche di marketing, visto che nessuno meglio di loro sa come sfruttare la paura del furto di identità per guadagnare. Il FACTA aveva anche obbligato le agenzie di credito a fornire ai cittadini americani un rapporto di credito gratuito una volta all'anno su richiesta. Grazie a tecniche di marketing ingannevoli, sono riuscite a trasformare questo requisito in un business da molti milioni di dollari.

Affidatevi a LifeLock se volete, o a uno dei suoi concorrenti se preferite. Ma ricordate che potete fare da soli molto di ciò che offrono queste compagnie. Potete inserire un avviso di frode nel vostro conto, ma dovete ricordarvi di rinnovarlo ogni tre mesi. Potete anche instaurare un congelamento del credito sul vostro conto, che è tutto lavoro in più per il cliente medio, ma molto efficace se siete dei precisini in fatto di privacy; e le norme cambiano di stato in stato. E forse un giorno il Congresso farà la cosa giusta e farà fallire LifeLock obbligando i prestatori a verificare l'identità di un individuo ogni volta che emettono un credito.

LifeLock:

<<http://www.lifelock.com>>

FACTA:

<<http://www.ftc.gov/opa/2004/06/factaidt.shtm>>

<<http://www.treasury.gov/offices/domestic-finance/financial-institution/cip/pdf/fact-act.pdf>>

oppure <<http://tinyurl.com/yqh9vh>>

Gli avvisi di frode:

<<http://www.consumersunion.org/creditmatters/creditmattersfactsheets/001626.html>>

oppure <<http://tinyurl.com/564hrn>>

L'articolo del New York Times:

<<http://www.nytimes.com/2008/05/24/business/yourmoney/24money.html?8dpc>>

Cause legali:

<<http://www.networkworld.com/news/2008/022108-credit-reporting-firm-sues-lifelock.html>>

oppure <<http://tinyurl.com/6dgoa3>>

<<http://www.insidetech.com/news/2148-id-protection-ads-come-back-to-bite-lifelock-pitchman>>

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

Furto di identità:

<<http://www.schneier.com/crypto-gram-0504.html#2>>

<<http://www.ftc.gov/opa/2007/11/idtheft.shtm>>

<<http://www.consumer.gov/sentinel/pubs/top10fraud2007.pdf>>

<<http://www.privacyrights.org/ar/idtheftsveys.htm#Jav2007>>

Rapporti di credito gratuiti:

<<http://www.annualcreditreport.com/>>

<[http://blog.washingtonpost.com/securityfix/2005/09/beware\\_free\\_credit\\_report\\_scam\\_1.html](http://blog.washingtonpost.com/securityfix/2005/09/beware_free_credit_report_scam_1.html)>

oppure <<http://tinyurl.com/66vjwk>>

<<http://www.msnbc.msn.com/id/7803368/>>

<<http://ezinearticles.com/?The-Free-Credit-Report-Scam&id=321877>>

Come difendersi:

<<http://www.nytimes.com/2008/05/24/business/yourmoney/24moneyside.html>>

<[http://www.savingadvice.com/blog/2008/06/04/102143\\_never-pay-someone-to-protect-your-identity.html](http://www.savingadvice.com/blog/2008/06/04/102143_never-pay-someone-to-protect-your-identity.html)>

oppure <<http://tinyurl.com/66ddv7>>

Questo articolo è originariamente apparso su Wired.com:

<[http://www.wired.com/politics/security/commentary/securitymatters/2008/06/securitymatters\\_0612](http://www.wired.com/politics/security/commentary/securitymatters/2008/06/securitymatters_0612)>

oppure <<http://tinyurl.com/3kkskp>>

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

Le news su Schneier/BT Counterpane

Intervista a Schneier in The Edge:

<[http://www.theledgedaily.com/cms/content.jsp?id=com.tms.cms.article.Article\\_71a20bfd-cb73c03a-18992130-695434f1](http://www.theledgedaily.com/cms/content.jsp?id=com.tms.cms.article.Article_71a20bfd-cb73c03a-18992130-695434f1)>

oppure <<http://tinyurl.com/5fw4su>>

Filmato di una tavola rotonda a cui Schneier ha partecipato a Supernova; l'argomento era la sicurezza e la privacy.

<<http://conversationhub.com/2008/07/10/session-video-privacy-and-security-in-the-network-age/>>

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

## Il primo Workshop interdisciplinare sulla Sicurezza e il comportamento umano

Qualche settimana fa, al MIT, è stato tenuto il primo Workshop interdisciplinare sulla Sicurezza e il comportamento umano (First Interdisciplinary Workshop on Security and Human Behavior - SHB 08). Dal sito Web:

“La sicurezza è sia una percezione che una realtà, e sono due cose differenti. Esistono svariate comunità di ricerca: tecnologi che studiano i sistemi di sicurezza, e psicologi che studiano le persone; senza contare gli economisti, gli antropologi e molti altri. Queste realtà stanno avvicinandosi sempre più.

“\*La progettazione della sicurezza è per sua natura psicologica, eppure molti sistemi ignorano questo fatto, e i bias cognitivi inducono le persone a calcolare erroneamente i rischi. Per esempio, l'icona di un lucchetto nell'angolo della finestra di un browser fa sentire le persone più al sicuro di quanto lo siano in realtà; mentre moltissime persone si sentono meno sicure quando viaggiano in aereo di quanto lo siano in realtà. Molti aggressori sfruttano a proprio vantaggio tali bias.

“\*Le problematiche di sicurezza riguardano i rischi e le incertezze, e i modi con cui si reagisce a essi. I bias cognitivi e percettivi alterano la maniera con cui trattiamo i rischi, e conseguentemente il modo di comprendere la sicurezza -- sia essa la sicurezza di una nazione, di un sistema di informazioni o dei propri dati personali.

“\*Molti attacchi veri e propri condotti contro sistemi di informazioni fanno leva più su aspetti psicologici che tecnologici. Gli attacchi di phishing ingannano le persone invitandole ad autenticarsi su siti Web che sembrano legittimi, ma che in realtà servono a rubare password. Contromisure di tipo tecnico possono contrastare certe tattiche di phishing, ma impedire agli utenti di prendere decisioni errate è molto più difficile.

“\*Per essere veramente efficace, la sicurezza deve essere usabile -- non solo dai nerd, ma dalla gente comune. La ricerca per una sicurezza usabile invariabilmente implica una componente psicologica.

“\*Il terrorismo viene percepito come una delle principali minacce per la società. Eppure i veri danni causati da attacchi terroristici non sono nulla in confronto agli effetti secondari che entrano in gioco quando le società prese di mira reagiscono in forma esagerata. Qui le questioni sono molte, dalla manipolazione della percezione dei rischi, all'antropologia della religione.

“\*Esistono domande fondamentali per la ricerca; per esempio, fino a che punto l'utilizzo e la scoperta dell'inganno nei contesti sociali possano aver contribuito a guidare l'evoluzione umana.

“Il dialogo fra i ricercatori nel campo della sicurezza e della psicologia si sta rapidamente allargando, coinvolgendo un numero sempre maggiore di discipline -- progettazione dell'usabilità della sicurezza, ideazione di protocolli, privacy e policy da un lato, e psicologia sociale, biologia evoluzionistica ed economia comportamentale dall'altro”.

Circa un anno fa, Ross Anderson e io concepimmo questa conferenza come un sistema per riunire ricercatori di sicurezza informatica, psicologi, economisti comportamentali, sociologi, filosofi e altri -- ognuno dei quali studia la parte umana della sicurezza. Ho letto molto, e scritto alcuni articoli, su psicologia e sicurezza in questi anni, e mi ha sempre molto impressionato la ricerca che specialisti al di fuori del mio settore hanno compiuto su argomenti profondamente legati al mio settore. Ross e io abbiamo pensato che sarebbe stato affascinante per tutti riunire queste comunità di ricercatori così diverse. Pertanto abbiamo convinto gli economisti comportamentali Alessandro Acquisti e George Loewenstein ad aiutarci a organizzare il workshop, abbiamo invitato tutti coloro di cui abbiamo letto gli studi, e in più abbiamo chiesto a costoro chi altri invitare. La risposta è stata grandiosa. La quasi totalità degli invitati ha potuto partecipare, e il risultato è stato una conferenza di 42 persone con 35 relatori, fra cui Nicholas Humphrey, Frank Furedi e James Randi.

<<http://www.cl.cam.ac.uk/~rja14/shb08.html>>

Agenda:

<<http://www.cl.cam.ac.uk/~rja14/shb08/agenda.html>>

Gli invitati e il loro lavoro:

<<http://www.cl.cam.ac.uk/~rja14/shb08/index.html>>

Sommari e appunti sugli interventi:

<<http://www.lightbluetouchpaper.org/2008/06/30/security-psychology/>>

<<http://www.ljean.com/files/SHBnotes.html>>

Registrazioni audio del workshop:

<<http://www.crypto.com/blog/shb08/>>

Foto:

<<http://www.cl.cam.ac.uk/~fms27/shb-2008/>>

<[http://www.lukechurchphotography.com/gallery/5341110\\_NYVVd#326538830\\_N3ELV](http://www.lukechurchphotography.com/gallery/5341110_NYVVd#326538830_N3ELV)>

oppure <<http://tinyurl.com/5t7r2c>>

Articoli sull'evento:

<<http://redtape.msnbc.com/2008/07/cambridge-mass.html>>

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

La verità sugli hacker cinesi

L'idea diffusa fra i media è che vi sia un'operazione coordinata da parte del governo cinese per effettuare hacking ai danni dei computer americani (dell'esercito, del governo, delle aziende) e rubarne i segreti. La verità è molto più complessa.

È indubbio che parecchio hacking stia fuoriuscendo dalla Cina. Qualsiasi azienda che si occupa di monitoraggio di sicurezza può vederlo continuamente.

Questi gruppi di hacker sembrano non lavorare per il governo cinese. Né sembrano coordinati dall'esercito cinese. Sono sostanzialmente composti da giovani cittadini cinesi patriottici che cercano di dimostrare di essere all'altezza di tutti gli altri. Oltre alle reti americane (che ai media piace menzionare), i loro bersagli comprendono anche siti pro-Tibet, pro-Taiwan, Falun Gong e pro-Uyghur.

Sono due i motivi che spingono tali hacker: la fama e la gloria, e il tentativo di vivere di questo mestiere. La fama e la gloria derivano dai loro obiettivi nazionalistici. Alcuni di questi hacker sono degli eroi in Cina. Mantengono alto l'onore del loro paese sia contro coalizioni anti-cinesi come il movimento pro-Tibet, sia contro grandi avversari come gli Stati Uniti.

E il denaro proviene dalle fonti più varie. I gruppi vendono i computer che riescono a penetrare, servizi di malware, e le informazioni che rubano sul mercato nero. Vendono strumenti per l'hacking e filmati ad altri che vogliono unirsi al gioco. Vendono persino T-shirt, berretti e altro merchandising sui loro siti Web.

Ciò detto, non è che l'esercito cinese ignori l'esistenza dei gruppi di hacker all'interno del paese. Di sicuro il governo cinese conosce i leader del movimento degli hacker e sceglie di guardare da un'altra parte. Probabilmente si rivolge a loro per comprare informazioni di intelligence rubate. Probabilmente recluta alcuni soggetti per le proprie organizzazioni scegliendoli in questo vivaio di hacker esperti e navigati. Di certo il governo impara dagli hacker.

E alcuni di quegli hacker sono in gamba. Negli anni, hanno raffinato i loro strumenti e le loro tecniche. Sono furtivi. Svolgono un'ottima ricognizione di rete. A mio avviso, quel che il Pentagono crede sia il problema, è in realtà solo una piccola parte del vero problema.

E scoprono da soli le proprie vulnerabilità. Qualche mese fa, un'azienda di sicurezza ha notato un attacco singolare contro un'organizzazione pro-Tibet. Quello stesso attacco era stato utilizzato due settimane prima contro una grande multinazionale fornitrice di servizi per la difesa.

Oltre a scoprire vulnerabilità, le accumulano e le conservano. Durante il conflitto del 1999 sulla teoria dei due stati, in un diverbio molto acceso con un gruppo di hacker taiwanesi, un gruppo cinese minacciò di scatenare un intero gruppo di worm allo stesso tempo. Non c'era motivo di non credere a tale minaccia.

Anzi, il fatto che questi gruppi non siano guidati dal governo cinese peggiora la situazione. Senza un coordinamento politico centrale, è probabile che gli hacker decidano di correre più rischi, compiano azioni più sconsiderate e in generale ignorino le conseguenze politiche delle loro bravate.

In quest'ottica, sono più che altro un attore non statale.

E quindi, se da un lato mi sta più che bene che il governo americano stia usando la minaccia degli hacker cinesi come stimolo a riorganizzare la propria sicurezza cibernetica (e spero che ci riesca), dall'altro spero che il governo americano riconosca che questi gruppi non stanno agendo sotto la direzione dell'esercito cinese e non tratti le loro azioni come ufficialmente approvate dal governo cinese.

Questo articolo è originariamente apparso sul sito Web di Discovery Channel:  
<<http://dsc.discovery.com/technology/my-take/computer-hackers-china.html>>  
oppure <<http://tinyurl.com/5lv3ac>>

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

## Attacchi man-in-the-middle

Il drammatico salvataggio di 15 ostaggi tenuti prigionieri dall'organizzazione di guerriglieri FARC avvenuto la scorsa settimana è stato il risultato di un intricato inganno che il governo colombiano ha portato avanti per mesi. Il piano si fondava sul classico concetto di attacco man-in-the-middle.

In un attacco man-in-the-middle, l'aggressore si inserisce fra due parti in comunicazione tra loro. Entrambe le parti credono di star comunicando fra loro, e l'aggressore può cancellare o modificare le comunicazioni a suo piacere. Il Wall Street Journal ha riferito come questo trucco abbia funzionato in Colombia:

"Il piano aveva buone speranze di riuscita perché per mesi -- in un'operazione che un ufficiale dell'esercito ha paragonato a un 'telefono rotto' -- l'intelligence militare era stata in grado di convincere il rapitore della signorina Betancourt, Gerardo Aguilar (un guerrigliero noto come 'Cesar'), che stesse comunicando con i suoi capi supremi del segretariato dei guerriglieri, composto da sette uomini. L'intelligence militare ha analogamente convinto i leader della guerriglia che stessero comunicando con Cesar. In realtà, entrambe le parti stavano parlando con l'intelligence militare".

Questo piano ha funzionato perché Cesar e i suoi capi guerriglieri non si conoscevano bene di persona. Non hanno riconosciuto le rispettive voci, e non avevano un'amicizia o una storia in comune che avrebbero potuto insospettirli. L'attacco man-in-the-middle viene sconfitto dal contesto, e i guerriglieri FARC ne erano privi.

Ed è per questo che l'attacco man-in-the-middle (abbreviato in MITM dalla comunità della sicurezza informatica) è un grave problema online: le comunicazioni via Internet sono spesso private di un contesto. Non esiste un modo per riconoscere il volto di qualcuno. Non esiste un modo per riconoscere la voce di qualcuno. Quando riceviamo un'email che sostiene di provenire da una certa persona o azienda, non abbiamo idea di chi l'abbia davvero spedita. Quando visitiamo un sito Web, non sappiamo se stiamo davvero visitando QUEL sito Web. A tutti piace fingere di sapere con chi stiamo comunicando -- e naturalmente, nella maggior parte dei casi, non vi è alcun aggressore a interferire con le nostre comunicazioni -- ma in realtà non lo sappiamo. Ed esistono svariati strumenti di hacking che sfruttano questa fiducia ingiustificata e che implementano attacchi MITM.

Anche in presenza di un contesto, è sempre possibile che il MITM inganni le due parti in causa, perché spesso le comunicazioni elettroniche sono intermittenti. Poniamo che uno dei guerriglieri FARC avesse cominciato a nutrire qualche sospetto nei confronti della persona con cui stava parlando. E che come prova gli avesse rivolto una domanda basata sulla loro storia in comune: "Che cosa abbiamo ordinato per cena l'anno scorso in quell'occasione?", o qualcosa del genere. Al telefono, l'aggressore non avrebbe

potuto rispondere velocemente, e l'inganno sarebbe stato scoperto. Ma una corrispondenza via email non è sincrona. L'aggressore potrebbe semplicemente far passare quella domanda all'altro capo della comunicazione, ascoltare la risposta, e quindi rispondere utilizzando le informazioni corrette.

Questo è il sistema con cui vengono lanciati gli attacchi MITM contro sistemi finanziari basati sul Web. Una banca richiede all'utente di autenticarsi con una password, con un codice unico ottenuto da un token, e simili. L'aggressore, che si trova fra le due parti, riceve la richiesta della banca e la passa all'utente. L'utente risponde all'aggressore, che passa tale risposta alla banca. A questo punto la banca dà per scontato di essere in comunicazione con l'utente legittimo, e l'aggressore è libero di inviare transazioni direttamente alla banca. Questo genere di attacco aggira completamente qualsiasi meccanismo di autenticazione a due fattori, e sta diventando una tattica di furto di identità sempre più diffusa.

Esistono soluzioni crittografiche contro gli attacchi MITM, ed esistono protocolli Web sicuri che le implementano. Molti di essi, tuttavia, richiedono segreti condivisi, pertanto si rivelano utili solamente in quelle situazioni in cui le persone già si conoscono e hanno reciproca fiducia.

I telefoni sicuri STU-III e STE, realizzati dalla NSA, risolvono il problema del MITM incorporando l'identità di ogni telefono nella sua chiave. (La NSA crea tutte le chiavi e ha la fiducia di tutti, per cui il sistema funziona). Quando due telefoni comunicano fra loro in forma sicura, si scambiano le chiavi e visualizzano su un display l'identità dell'altro telefono. Dato che l'apparecchio si trova in un luogo sicuro, l'utente a quel punto sa con chi sta parlando, e se il telefono visualizzasse un'altra organizzazione (come avverrebbe in caso di attacco MITM), l'utente interromperebbe la chiamata.

Zfone, un sistema di VoIP sicuro, protegge dagli attacchi MITM grazie a una breve stringa di autenticazione. Dopo che due terminali Zfone si scambiano le chiavi, entrambi i computer visualizzano una stringa di quattro caratteri. Gli utenti devono quindi verificare manualmente l'identità di entrambe le stringhe -- "Sul mio schermo c'è scritto 5C19; il tuo che cosa dice?" -- per assicurarsi che i telefoni stanno davvero comunicando direttamente e non con un MITM. Il modello TSD-3600 di AT&T funzionava in maniera analoga.

Questo tipo di protezione è integrata in SSL, ma nessuno la usa. Per come viene utilizzato normalmente, SSL fornisce un link di comunicazione criptato a chiunque si trovi dall'altra parte, che sia una banca o un sito di phishing. E i migliori siti di phishing creano connessioni SSL valide, per ingannare gli utenti in modo ancora più efficace. Ma se l'utente volesse, potrebbe controllare manualmente il certificato SSL per vedere se è stato emesso alla "Banca Nazionale della Fiducia" o a "Due Tizi con un Computer in Nigeria".

Nessuno lo fa, però, perché occorre tenerlo a mente ed essere disposti a rimboccarsi le maniche. (I browser, se volessero, potrebbero facilitare questa operazione, ma apparentemente non vogliono). Nel mondo reale è facile distinguere tra una filiale della propria banca e un cambiatore di valuta all'angolo della strada. Ma su Internet un sito di phishing può facilmente essere confezionato per sembrare identico a quello della banca. Ogni metodo per riuscire a distinguerli richiede uno sforzo. E questo è il primo passo per ingannare qualcuno con un attacco MITM.

Man-in-the-middle non è un attacco nuovo, e non deve necessariamente basarsi sulla tecnologia. Ma Internet facilita gli attacchi e li rende più potenti, e non è una tendenza destinata a cambiare tanto presto.

L'articolo del Wall Street Journal:

<<http://online.wsj.com/article/SB121518490923829025.html>>

Gli strumenti di hacking MITM:

<<http://www.monkey.org/~dugsong/dsniff/>>

<<http://www.oxid.it/>>

<<http://ettercap.sourceforge.net/>>

<<http://sourceforge.net/projects/airjack/>>

<<http://www.wsniiff.com/>>

<<http://www.theta44.org/karma/>>

Problemi dell'autenticazione a due fattori:

<<http://www.schneier.com/crypto-gram-0503.html#2>>

I telefoni sicuri della NSA:

<<http://www.fas.org/irp/program/security/work/stu3.html>>

Zfone:

<<http://zfoneproject.com/faq.html#mitm>>

AT&T TSD 3600:

<<http://www.flickr.com/photos/21746901@N08/2275723713/>>

Controllare i certificati SSL:

<<http://www.microsoft.com/protect/yourself/phishing/spoof.msp>>

Questo articolo è originariamente apparso su Wired.com:

<[http://www.wired.com/politics/security/commentary/securitymatters/2008/07/securitymatters\\_0710](http://www.wired.com/politics/security/commentary/securitymatters/2008/07/securitymatters_0710)>

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

Commenti dei lettori

Su questi argomenti vi sono centinaia di commenti nel mio blog, molti davvero interessanti. Cercate l'argomento sul quale intendete dare la vostra opinione, e unitevi al dibattito.

<<http://www.schneier.com/blog>>

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

CRYPTO-GRAM è una newsletter mensile gratuita che offre riassunti, analisi, approfondimenti, e commenti sulla sicurezza (informatica e in generale) e sulla crittografia. I numeri arretrati sono disponibili all'indirizzo

<<http://www.schneier.com/crypto-gram.html>>. Per iscriversi, cancellare l'iscrizione o cambiare il proprio indirizzo a cui recapitare la newsletter, visitate sempre <<http://www.schneier.com/crypto-gram.html>>

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](mailto:crypto-gram@communicationvalley.it)>

I commenti a CRYPTO-GRAM devono essere inviati a [schneier@counterpane.com](mailto:schneier@counterpane.com). Si sottintende il permesso di riprodurre tali commenti, salvo indicazione contraria. I commenti possono venire adattati per ragioni di spazio e di chiarezza.

Inoltrate liberamente CRYPTO-GRAM a colleghi ed amici che possano trovare questa pubblicazione di un certo interesse. Viene concessa l'autorizzazione a ristampare CRYPTO-GRAM, a condizione che sia stampata integralmente.

CRYPTO-GRAM è realizzata da Bruce Schneier. Schneier è l'autore dei best seller "Beyond Fear", "Secrets and Lies" [tradotto in Italia col titolo "Sicurezza Digitale"] e "Applied Cryptography", e inventore degli algoritmi Blowfish, Twofish e Yarrow. È il fondatore e CTO di BT Counterpane e membro del comitato consultivo dell'Electronic Privacy Information Center (EPIC). Frequentemente scrive e partecipa a conferenze sulla sicurezza informatica e sulla crittografia. Il suo sito Web è all'indirizzo <<http://www.schneier.com>>.

BT Counterpane è leader mondiale nella protezione delle informazioni su network - l'inventore del Managed Security Monitoring gestito in outsourcing e la principale autorità nella riduzione efficace delle nuove minacce in ambito IT. BT Counterpane protegge reti per conto di governi e di aziende inserite nella Fortune 1000 a livello mondiale.

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

Crypto-Gram è una newsletter personale. Le opinioni qui espresse non sono necessariamente quelle di BT o di BT Counterpane.

Copyright (c) 2008 - Bruce Schneier.