

CRYPTO-GRAM
15 marzo 2009

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:

- Incentivi di sicurezza perversi
- La privacy nell'epoca della persistenza
- News
- Gli insider
- Il Canile: Singularics
- Tre aneddoti di sicurezza dal mondo degli insetti
- La gentilezza degli sconosciuti
- Nuova frode su eBay
- Le news su Schneier
- Sicurezza IT: incolpare la vittima
- Bilanciare sicurezza e usabilità nei processi di autenticazione
- Commenti dei lettori

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

Incentivi di sicurezza perversi

Un dipendente della catena Whole Foods ad Ann Arbor, Michigan, fu licenziato nel 2007 per aver fermato un taccheggiatore. Nello specifico, fu licenziato per aver toccato un cliente, non importa se quel cliente aveva uno zaino pieno di generi alimentari rubati e stava scappando con tutta quella merce.

Mi capita in continuazione di notare decisioni di sicurezza che, come nell'episodio accaduto a Whole Foods, sembrano totalmente prive di senso. Tuttavia in ognuno di questi casi in realtà le decisioni prese acquistano senso una volta compresi gli incentivi che le guidano. Tutte le decisioni di sicurezza sono compromessi, ma le ragioni dietro di esse non sempre risultano ovvie. Spesso sono soggettive e spinte da incentivi esterni. E altrettanto spesso dei compromessi di sicurezza vengono messi in atto per motivi non strettamente legati alla sicurezza.

Quasi certamente Whole Foods ha una policy 'non toccate il cliente' dietro consiglio dei suoi avvocati. Il 'non toccare' è anche una misura di sicurezza, ma si tratta di sicurezza contro possibili cause legali intentate dai clienti. Il costo di tali cause legali sarebbe molto, molto maggiore dei 346 dollari di merce rubata in questo caso. Anche nel caso di sospetti taccheggiatori, la policy ha senso: il costo di una causa derivata dall'aver fermato per sbaglio un cliente innocente sarebbe molto maggiore di quanto costerebbe lasciar fuggire i taccheggiatori. Per perverso che sembri, il risultato è del tutto ragionevole se consideriamo gli incentivi aziendali -- Whole Foods ha adottato una policy aziendale a proprio beneficio.

Almeno, funziona fin quando la polizia e altri fattori mantengono il numero dei taccheggiatori a un livello ragionevolmente basso.

Gli incentivi spiegano parecchio di quel che può lasciare perplessi su certi compromessi di sicurezza. Perché King County, stato di Washington, richiede una sola forma di identificazione per l'ottenimento di un porto d'armi, ma due forme di identificazione per poter pagare il porto d'armi con un assegno? Commettere un errore su un permesso del genere è un problema astratto, mentre un assegno scoperto o falso è una reale perdita di denaro per il dipartimento.

Nei decenni precedenti l'11 settembre, perché le compagnie aeree erano contrarie a ogni misura di sicurezza tranne il controllo di documenti d'identità con foto? Maggiori controlli di sicurezza indispongono i clienti, ma il controllo dei documenti d'identità risolveva un problema di sicurezza di altro genere: la rivendita dei biglietti non rimborsabili. E quindi alle compagnie aeree andava bene quel tipo di controllo.

E per quale motivo la TSA sequestra i liquidi ai checkpoint di sicurezza, nella remota possibilità che un terrorista cerchi di realizzare un esplosivo liquido invece di utilizzare i più comuni esplosivi solidi? Perché i funzionari a cui spettava compiere la decisione si sono serviti di misure di sicurezza 'per pararsi il didietro' mirate a tattiche specifiche e conosciute, invece che a tattiche più generiche e ad ampio raggio.

Gli stessi distorti incentivi spiegano il continuo problema di prigionieri innocenti costretti a passare anni in luoghi come Guantanamo e Abu Ghraib. La soluzione sembrerebbe ovvia: rilasciare gli innocenti, trattenere i colpevoli, e cercare di scoprire chi è innocente e chi è colpevole fra coloro di cui non abbiamo certezza. Ma gli incentivi sono più perversi di tutto questo. Chi firmerà l'ordine di rilascio di uno di quei prigionieri? Quale ufficiale militare accetterà il rischio di fare una mossa sbagliata, non importa quanto piccolo sia tale rischio?

Circa cinque anni fa ho letto che i prigionieri venivano tratti dagli Stati Uniti molto più a lungo del dovuto, perché "nessuno voleva essere responsabile del rilascio del prossimo Osama bin Laden". Quell'incentivo a non fare nulla non è cambiato. Anzi, potrebbe persino essersi rafforzato, guardando come questi poveretti appassiscono in galera.

In tutti questi casi il sistema migliore per cambiare il compromesso è cambiare gli incentivi. Osserviamo come funziona il caso Whole Foods. I dipendenti del negozio non devono arrestare i taccheggiatori perché la società ha creato un'organizzazione speciale appositamente autorizzata a fermare quelle persone che il negozio segnala come taccheggiatori -- quest'organizzazione è la polizia. Se vogliamo che la TSA si comporti in maniera più razionale, deve esservi qualcuno con una prospettiva più ad ampio raggio disposto a confrontarsi con minacce più generali invece di concentrarsi su bersagli o tattiche particolari.

Per quanto riguarda i prigionieri, la società ha creato un'organizzazione speciale a cui ha appositamente affidato il ruolo di giudicare le prove contro di essi e rilasciarli se è il caso -- quest'organizzazione è la magistratura, il potere giudiziario. È soltanto perché l'amministrazione di George W. Bush ha deciso di togliere i prigionieri di Guantanamo dal sistema legale che adesso ci ritroviamo questi incentivi perversi. Il nostro paese farebbe una mossa intelligente se riportasse il maggior numero possibile di queste persone all'interno del sistema legale.

Questo articolo è originariamente apparso su Wired.com.

<http://www.wired.com/politics/security/commentary/securitymatters/2009/02/securitymatters_0226>

oppure <<http://tinyurl.com/aku6bf>>

L'incidente Whole Foods:

<http://www.mlive.com/news/index.ssf/2007/12/grocery_worker_fired_for_stopp.html>

oppure <<http://tinyurl.com/3dma49>>

I controlli di identificazione di King County:

<<http://www.kingcounty.gov/safety/sheriff/Services/Gun.aspx>>

Terroristi ed esplosivi liquidi:

<http://www.schneier.com/blog/archives/2007/08/details_on_the_1.html>

Sicurezza 'per pararsi il didietro':

<http://www.schneier.com/blog/archives/2007/02/cya_security_1.html>

Gli incentivi perversi del mantenere sotto custodia i sospetti terroristi:

<<http://query.nytimes.com/gst/fullpage.html?res=9C00E3DF133EF934A15756C0A9629C8B63&sec=&spon=&pagewanted=all>>

oppure <<http://tinyurl.com/cqh86n>>

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

La privacy nell'epoca della persistenza

(Nota: Non è la prima volta che ho affrontato questo argomento, e non sarà di certo l'ultima. Stavolta mi sembra di aver fatto un ottimo riassunto delle problematiche, ed è per questo che ripubblico l'articolo).

Benvenuti nel futuro, dove ogni cosa che vi riguarda viene registrata. Un futuro dove le vostre azioni sono registrate, i vostri movimenti tracciati, e le conversazioni non sono più effimere. Un futuro che non giunge a voi partendo da chissà quale distopia nello stile di "1984", ma dalla tendenza naturale dei computer di produrre informazioni.

I dati personali sono l'inquinamento dell'era dell'informazione. Sono il sottoprodotto naturale di ogni interazione mediata da un computer. Rimangono in circolazione finché non vengono smaltiti. Hanno valore se riutilizzati, ma occorre farlo con attenzione. Altrimenti i suoi effetti collaterali sono tossici.

E allo stesso modo in cui cent'anni fa la gente non si curava dell'inquinamento nella corsa alla realizzazione dell'Era Industriale, oggi non ci curiamo delle informazioni nella corsa alla realizzazione dell'Era dell'Informazione.

In misura sempre maggiore lasciamo ogni giorno una scia di 'impronte digitali virtuali' dietro di noi. Una volta si andava in libreria e si comprava un libro pagandolo in contanti. Ora si visita Amazon, e tutto quel che cerchiamo e compriamo viene registrato. Una volta si pagava il biglietto del treno con qualche moneta, ora abbiamo un biglietto elettronico collegato al nostro conto in banca. Le tessere cliente dei negozi ci offrono degli sconti; i commercianti utilizzano i dati delle tessere per risalire alle nostre abitudini di shopping.

Vengono raccolti dati che ci riguardano ogni volta che facciamo una telefonata, inviamo un'email, acquistiamo qualcosa con la carta di credito o visitiamo un sito Web. Una carta d'identità nazionale non farà altro che aggravare tutto questo.

Un numero sempre maggiore di sistemi computerizzati ci sta osservando. In alcune città le telecamere di sorveglianza sono dappertutto, e fra non molto la tecnologia di riconoscimento facciale sarà in grado di identificare le persone. Scanner automatici di targhe tengono traccia dei veicoli nei parcheggi e nelle città. Stampanti a colori, fotocamere digitali, e certe macchine fotocopiatrici sono dotate di codici di identificazione incorporati. La sorveglianza aerea viene utilizzata dalle città per rilevare abusi edilizi e dai commercianti per conoscere le dimensioni delle case e dei giardini.

E quando i chip RFID saranno più diffusi, verranno tracciati anch'essi. Già è possibile essere rintracciati grazie al nostro cellulare, anche se non facciamo chiamate. Questa è la sorveglianza all'ingrosso: non si tratta di "seguire quell'auto", ma di "seguire tutte le auto".

I computer stanno mediando anche le conversazioni. Le conversazioni faccia a faccia sono effimere. Anni fa, le compagnie telefoniche avrebbero potuto sapere chi avevamo chiamato e quanto tempo era durata la telefonata, ma non quel che si era detto in quella conversazione. Oggi si chiacchiera anche via email, mediante SMS, e sui siti di

social networking. Oggi scriviamo sui nostri blog e usiamo Twitter. Queste conversazioni -- con familiari, amici e colleghi -- possono essere registrate e archiviate.

Una volta era costoso archiviare queste informazioni, ma con la progressiva diminuzione del costo della memoria dei calcolatori, e con il diminuire dei costi di elaborazione, una sempre maggior quantità di tali dati viene diversamente indicizzata e correlata, per poi venire impiegata con secondi fini. Quel che una volta era effimero, oggi permane.

Chi può raccogliere e utilizzare queste informazioni viene stabilito dalle leggi locali. Negli Stati Uniti sono principalmente le grandi aziende a raccogliere, per poi comprare e vendere, molte di tali informazioni a scopi commerciali. In Europa sono più i governi a raccogliere questi dati che non le aziende. In entrambi i continenti le forze dell'ordine vogliono poter accedere alla maggior quantità possibile di tali informazioni, a scopi investigativi e per effettuare data mining.

In tutti i paesi, sempre più organizzazioni stanno raccogliendo, archiviando e condividendo una quantità sempre maggiore di questi dati.

E non finisce qui. Programmi e dispositivi di keyboard logging possono già registrare tutto quel che dattilosciviamo; ed è solo questione di pochi anni, poi si potrà registrare tutto quel che diciamo al cellulare.

Un piccolo "registratore vitale" da appuntare al bavero della giacca che registra di continuo quel che vediamo e sentiamo non è molto lontano. Verrà venduto come dispositivo di sicurezza, in modo che nessuno possa attaccarvi senza essere registrato. Quando questo oggetto sarà realtà, il non indossarlo verrà usato come prova che una persona intende commettere un reato, nella stessa maniera in cui oggi in tribunale l'accusa si serve del fatto che una persona ha lasciato il proprio cellulare a casa come prova che questi non voleva essere rintracciato?

Stiamo vivendo in un'epoca unica nella storia: la tecnologia esiste, ma non è ancora fluidamente integrata. I controlli di identità sono comuni, ma dobbiamo ancora mostrare i documenti. Presto la cosa avverrà in automatico, tramite un chip RFID nel portafoglio oppure mediante videocamere con riconoscimento facciale.

E quelle videocamere, oggi ancora visibili, si rimpiccioliranno al punto da scomparire. La conversazione effimera praticamente sparirà e la considereremo una cosa normale. Già adesso i nostri figli vivono molta più della loro vita in pubblico rispetto a noi. Il nostro futuro non ha privacy, non per effetto di strane tendenze governative verso lo stato di polizia, o a causa di condotte illecite aziendali, ma perché i computer producono, per loro natura, informazioni.

Il Cardinale Richelieu disse mirabilmente: "Datemi sei righe scritte dall'uomo più onesto, e ci troverò qualcosa per farlo impiccare". Quando tutte le nostre parole e azioni possono venire registrate per essere analizzate in un secondo momento, è necessario applicare regole diverse.

La società funziona proprio perché la conversazione è qualcosa di effimero; perché le persone dimenticano, e perché le persone non devono giustificare ogni parola proferita.

La conversazione non equivale alla corrispondenza. Parole dette di fretta mentre si prende un caffè la mattina, che vengano proferite in una caffetteria o scritte su un BlackBerry, non sono pronunciamenti ufficiali. Un pattern di informazioni che indica "tendenze terroristiche" non può sostituire un'indagine vera e propria. Essere sottoposti continuamente a controlli è una minaccia per i nostri costumi sociali; senza contare che dà i brividi. Privacy non vuol dire soltanto aver qualcosa da nascondere: ha invece un enorme valore per la democrazia, la libertà e la nostra essenziale umanità.

Non potremo mai fermare l'avanzamento tecnologico, così come non possiamo tornare a prima dell'invenzione dell'automobile o dei forni a carbone. Abbiamo passato l'era industriale affidandoci a combustibili fossili che hanno inquinato l'atmosfera e modificato il clima. Ora stiamo cercando di affrontare le conseguenze (sempre facendo uso di quei combustibili fossili, naturalmente). Magari questa volta potremmo essere un po' più proattivi.

Proprio come noi oggi guardiamo agli inizi del secolo scorso e ci sembra incredibile che quelle persone potessero ignorare tutto l'inquinamento che causavano, le generazioni future volgeranno il loro sguardo a noi, a queste prime decadi dell'era dell'informazione, e giudicheranno le nostre soluzioni per affrontare la proliferazione dei dati.

Dobbiamo iniziare a discutere, tutti insieme, questo importante cambiamento sociale e le sue implicazioni. E dobbiamo trovare un sistema per creare un futuro del quale i nostri nipoti andranno fieri.

Questo articolo è originariamente apparso sul sito Web BBC.com.
<<http://news.bbc.co.uk/1/hi/technology/7897892.stm>>

Documenti d'identità nazionali:
<<http://www.schneier.com/essay-160.html>>

Telecamere di sorveglianza:
<<http://www.schneier.com/essay-225.html>>

Chip RFID:
<<http://epic.org/privacy/rfid/>>

Sorveglianza attraverso i cellulari:
<<http://computerworld.com/action/article.do?command=viewArticleBasic&articleId=9127462>>
oppure <<http://tinyurl.com/au2f4n>>

Sorveglianza all'ingrosso:
<<http://www.schneier.com/essay-147.html>>

Data mining:
<<http://www.schneier.com/essay-108.html>>

Il futuro della sorveglianza:

<<http://www.schneier.com/essay-109.html>>

Riconoscimento facciale:

<<http://epic.org/privacy/facerecognition/>>

La privacy e i più giovani:

<<http://nymag.com/news/features/27341/>>

Effetti negativi di una sorveglianza costante:

<http://news.bbc.co.uk/1/hi/uk_politics/7872425.stm>

Il valore della privacy:

<<http://www.schneier.com/essay-114.html>>

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

News

Per vendere la propria penna indelebile, Uni-Ball si serve della paura, ma si tratta della paura sbagliata. Confondono la frode del riciclaggio di assegni, che avviene quando qualcuno prende un assegno e cambia il nome del beneficiario e magari anche l'ammontare della somma, con il furto di identità. E come può qualcuno rubarmi del denaro cancellando e modificando informazioni su un modulo fiscale? È un tentativo di far spedire l'assegno di rimborso a un altro indirizzo? È tutto tremendamente complicato.

<http://videogum.com/archives/commercials/s-epatha-merkerson-will-terrif_045001.html>

oppure <<http://tinyurl.com/7jcfu1>>

<http://www.schneier.com/blog/archives/2007/09/using_fear_to_s.html>

Los Alamos ha perso 80 computer: non si sa se sono stati rubati o se sono stati collocati nel luogo sbagliato. Classica vicenda, che non varrebbe nemmeno la pena di commentare, ma questo fantastico passaggio la dice molto lunga su ciò che non va bene della loro policy di sicurezza: "La lettera, indirizzata ai funzionari di sicurezza del Dipartimento per l'Energia sostiene che 'le misure di sicurezza cibernetica non sono state messe in atto con sufficiente puntualità' perché la perdita dei computer è stata trattata come un 'problema di gestione della proprietà'". Il vero rischio nei casi di perdita di computer sono i dati, non l'hardware. Credevo che tutti lo sapessero.

<<http://www.google.com/hostednews/afp/article/ALeqM5jXipyZU1GKO4KQ3f4hhKyLvJvTA>>

oppure <<http://tinyurl.com/d7oxy5>>

Le cose difficili da pronunciare sono considerate più rischiose di quelle facili da pronunciare:

<<http://www.ncbi.nlm.nih.gov/pubmed/19170941>>

Un nuovo studio: "WiFi networks and malware epidemiology" (Reti Wi-Fi ed epidemiologia del malware), di Hao Hu, Steven Myers, Vittoria Colizza e Alessandro

Vespignani. In tutta onestà, non sono sicuro di aver capito molto dell'articolo. E non credo che il loro modello sia tanto efficace. Ma mi piace vedere questo genere di metodi applicati al malware e all'andamento delle infezioni.

<<http://www.pnas.org/content/early/2009/01/26/0811973106>>

<<http://arxiv.org/abs/0706.3146>>

Responsabilità HIPAA nel piano di stimolo economico USA, ora diventato legge:

<http://www.schneier.com/blog/archives/2009/02/hipaa_accountab.html>

Una lezione di buonsenso sul terrorismo da parte dell'MI6:

<http://www.theregister.co.uk/2009/02/11/mi6_spy_rubbishes_terrorism_fear/>

oppure <<http://tinyurl.com/cxfl8s>>

Ecco un'analisi di 30.000 password prese da phpbb.com.

<http://www.darkreading.com/blog/archives/2009/02/phpbb_password.html>

È simile alla mia analisi di 34.000 password di MySpace.

<http://www.schneier.com/blog/archives/2006/12/realworld_passw.html>

Pare che non siamo tuttora in grado di scegliere delle password efficaci. Conficker.B sfrutta questa vulnerabilità, provando circa 200 password comuni per cercare di propagarsi sempre più.

<<http://www.sophos.com/blogs/gc/g/2009/01/16/passwords-conficker-worm/>>

Sul mio blog:

<http://www.schneier.com/blog/archives/2009/02/another_passwor.html>

Prova dell'efficacia della 'teoria delle finestre rotte' nella lotta al crimine:

<http://www.boston.com/news/local/massachusetts/articles/2009/02/08/breakthrough_on_broken_windows/>

oppure <<http://tinyurl.com/cslqo5>>

<<http://www.ncjrs.gov/App/publications/Abstract.aspx?id=246202>>

La NSA vuole contribuire all'intercettazione di comunicazioni via Skype:

<http://www.theregister.co.uk/2009/02/12/nsa_offers_billions_for_skype_pwnage/>

oppure <<http://tinyurl.com/a9hn2n>>

Sono certo si tratti di un problema reale. Ecco un articolo che sostiene che i malviventi italiani utilizzano Skype più del telefono proprio per evitare intercettazioni.

<http://www.theregister.co.uk/2009/02/16/italian_crooks_skype/>

Uno studio proveniente dal New Jersey dimostra che la Legge di Megan -- una legge pensata per identificare gli aggressori sessuali presso le comunità in cui vivono -- è inefficace sia nella riduzione di reati sessuali, sia come deterrente nei confronti dei recidivi.

<http://www.nj.com/news/index.ssf/2009/02/study_finds_megans_law_fails_t_1.html

>

oppure <<http://tinyurl.com/b2mql2>>

Un'altra variante di Conficker: Conficker B++. Si tratta di un malware ottimamente progettato.

<http://www.schneier.com/blog/archives/2009/02/new_conficker_v.html>

Il presidente Obama ha affidato a Melissa Hathaway il compito di condurre un'analisi di 60 giorni delle policy di sicurezza cibernetica nazionale.

<http://www.usatoday.com/tech/2009-02-16-cybersecurity-expert-obama_N.htm>

oppure <<http://tinyurl.com/cx3kon>>

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9127682&intsrc=news_ts_head>

oppure <<http://tinyurl.com/d2ygpp>>

Questa intervista dello scorso anno vi darà un'idea piuttosto precisa di come sia il modo di pensare di Hathaway.

<<http://www2.computer.org/portal/web/computingnow/1208/whatsnew/securityandprivacy>>

oppure <<http://tinyurl.com/by2817>>

Un tizio del Maine prova a costruire una 'bomba sporca' e a nessuno importa, probabilmente perché il tizio non è musulmano. Il terrorismo per la supremazia della razza bianca evidentemente non è molto in voga oggi.

<<http://jonathanstray.com/maine-man-tries-to-build-dirty-bomb>>

Si dice che esistano dei prototipi di granate a impulsi elettromagnetici:

<http://www.theregister.co.uk/2009/02/12/electropulse_grenades/>

TrapCall è un nuovo servizio che rivela il numero del chiamante in caso di chiamate anonime o con numero occultato.

<<http://blog.wired.com/27bstroke6/2009/02/trapcall.html>>

Un giudice ordina all'imputato di decriptare il proprio portatile: un caso da Quinto Emendamento molto interessante.

<http://news.cnet.com/8301-13578_3-10172866-38.html>

Usate questo specchio per doccia con telecamera nascosta per scoprire gli amanti di coniugi adulteri:

<<http://www.dpl-surveillance-equipment.com/100611.html>>

Il sito offre tutta una serie di telecamere nascoste negli oggetti domestici più comuni.

<http://www.dpl-surveillance-equipment.com/wireless_hidden_cameras.html>

Il professor Michael Fromkin dell'Università di Miami parla di società e documenti di identità in "Identity Cards and Identity Romanticism" (Carte di identità e romanticismo dell'identità).

<http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1309222>

<http://www.schneier.com/blog/archives/2009/03/michael_froomki.html>

Questo commento sulla strategia di sicurezza nazionale del governo inglese è allarmante: "Sir David Ormand, l'ex coordinatore della sicurezza e dell'intelligence di Whitehall, espone un piano del sistema con cui lo stato raccoglierà le informazioni -- comprese le informazioni di viaggio, i registri delle chiamate e della posta elettronica -- conservate da enti pubblici e privati, e ammette che 'Per scoprire i segreti altrui si dovranno infrangere le regole morali quotidiane'". In sostanza: è immorale, ma lo faremo comunque.

<<http://www.guardian.co.uk/uk/2009/feb/25/personal-data-terrorism-surveillance>>

oppure <<http://tinyurl.com/c5ll6r>>

I programmi "staple" e "unstaple" (lett. "graffettare" e "togliere le graffette") effettuano un tipo di crittografia tutto-o-nulla. È solo codice dimostrativo, ma ugualmente interessante.

<<http://sysnet.ucsd.edu/projects/staple/>>

Uno studio interessante: "Optimised to Fail: Card Readers for Online Banking" (Ottimizzati per sbagliare: i lettori di schede per il banking online), di Saar Drimer, Steven J. Murdoch e Ross Anderson.

<<http://www.cl.cam.ac.uk/~sjm217/papers/fc09optimised.pdf>>

<<http://www.lightbluetouchpaper.org/2009/02/26/optimised-to-fail-card-readers-for-online-banking/>>

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

Sono sicuro che occorre una certa abilità per poter usare questa penna da autodifesa, e sono altrettanto certo che passerà senza problemi qualsiasi checkpoint di sicurezza.

<<http://www.botachtactical.com/kzxtremepen.html>>

Questo articolo offre una panoramica sui robot dell'esercito statunitense, e parla di alcune delle problematiche legate all'etica del loro utilizzo in guerra.

<<http://www.thenewatlantis.com/publications/military-robots-and-the-laws-of-war>>

oppure <<http://tinyurl.com/csoj98>>

L'articolo è stato adattato dal suo libro "Wired for War: The Robotics Revolution and Conflict in the 21st Century" (Predisposti alla guerra: la rivoluzione robotica e il conflitto nel XXI Secolo), pubblicato quest'anno. Ho acquistato il libro, ma non l'ho ancora letto. Sempre sull'argomento, vi è questo studio sull'etica dei robot militari autonomi.

<http://www.schneier.com/blog/archives/2008/01/ethics_of_auton.html>

Sul mio blog:

<http://www.schneier.com/blog/archives/2009/03/history_and_eth.html>

Una fuga di documenti segreti della NATO sulla guerra in Afghanistan, dovuta a una password debole:

<<https://secure.wikileaks.org/wiki/N1>>

Allarmismo terroristico e messinscena di sicurezza in alberghi e chiese:

<<http://news.bbc.co.uk/1/hi/england/london/7933004.stm>>

<<http://www.cnn.com/2009/CRIME/03/09/church.security/index.html>>

<http://www.schneier.com/blog/archives/2009/03/security_theate_2.html>

Affascinante storia delle tecniche utilizzate per distribuire materiale pedopornografico in tutto il mondo:

<http://wikileaks.org/wiki/My_life_in_child_porn>

<http://www.schneier.com/blog/archives/2009/03/the_techniques.html#c356628>

oppure <<http://tinyurl.com/asnc63>>

Spam su Google Maps:

<http://www.schneier.com/blog/archives/2009/03/google_map_spam.html>

Questa storia del furto del più grande diamante al mondo sembra la trama di un film:

<http://www.wired.com/politics/law/magazine/17-04/ff_diamonds?currentPage=all>
oppure <<http://tinyurl.com/ak8hrx>>

Molti tastierini Sentex, utilizzati per proteggere porte e ingressi un po' dappertutto, possono venire aperti con una password di amministratore di default:
<http://www.schneier.com/blog/archives/2009/03/the_doghouse_se_1.html>

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

Gli insider

Rajendrasinh Makwana lavorava come sistemista UNIX autonomo per Fannie Mae. Il 24 ottobre scorso è stato licenziato. Prima di andarsene ha inserito una bomba logica all'interno della rete dell'organizzazione. La bomba sarebbe stata 'detonata' il 31 gennaio. Era programmata per disabilitare l'accesso al server sul quale era stata installata, bloccare qualsiasi software di monitoraggio di rete, cancellare tutte le informazioni sistematicamente e in maniera irrecuperabile, per poi autoreplicarsi su tutti i 4.000 server di Fannie Mae. Secondo la documentazione presentata in tribunale, il costo dei danni sarebbe stato nell'ordine dei milioni di dollari, una cifra che appare comunque bassa. Fannie Mae avrebbe dovuto chiudere per almeno una settimana.

Per fortuna (e sembra proprio che si tratti di pura fortuna), una settimana dopo un altro programmatore ha scoperto lo script e lo ha disattivato.

Gli insider sono un eterno problema. Hanno accesso al sistema e vengono riconosciuti dal sistema. Sanno come funziona il sistema, la sua sicurezza e i suoi punti deboli. Hanno l'opportunità di agire quando vogliono. I grandi colpi alle banche, le rapine ai casinò, le frodi aziendali su vasta scala, le rapine ai treni: in molte delle operazioni criminali più impressionanti sono coinvolti gli insider (ossia persone che lavorano all'interno di un'azienda). E, come dimostra il tentativo di vendetta di Makwana, questi insider possono avere dei moventi piuttosto forti, che possono solo intensificarsi se l'economia continua a soffrire e aumenta il numero dei licenziamenti.

Gli insider sono aggressori particolarmente pericolosi perché sono persone fidate. Hanno accesso perché CI SI ASPETTA che lo abbiano. Hanno libertà d'azione e conoscono il sistema perché lo usano, oppure perché lo hanno progettato, costruito o installato. Si trovano già all'interno del sistema di sicurezza, per cui è molto più difficile difendersi contro di loro.

Non è possibile progettare un sistema senza persone fidate. Esistono dappertutto. Negli uffici, gli impiegati sono persone fidate a cui si dà accesso a strutture e risorse, e che hanno il permesso (a volte ad ampio raggio, altre volte con una serie di restrizioni) di agire in nome dell'azienda. Nei negozi, i dipendenti possono andare nel retro e avere accesso al registratore di cassa; e i clienti possono entrare nel negozio e toccare la merce. Ai dipendenti dell'IRS (l'Ufficio Tasse americano) vengono affidate informazioni fiscali personali; ai dipendenti di un ospedale si affidano le informazioni mediche dei pazienti. Le banche, gli aeroporti, i penitenziari, sono tutte strutture che non potrebbero funzionare senza persone di fiducia.

Mettere dei computer al posto delle persone fidate non risolve il problema: semplicemente lo sposta e lo rende ancor più complesso. Il computer, il software, i progettisti della rete, chi l'ha installata, chi l'ha programmata e chi la mantiene, ecc., sono tutte persone fidate. Basta osservare qualunque analisi della sicurezza delle macchine per il voto elettronico, o alcune delle frodi perpetrate ai danni di macchine per il gioco d'azzardo, per avere alcuni esempi grafici dei rischi legati alla sostituzione di persone con delle macchine.

Ovviamente questo problema esiste da molto più tempo dei computer. E le soluzioni non sono cambiate granché nella storia. Esistono cinque tecniche di base per gestire persone fidate:

1. Limitare il numero di persone fidate. E questo è ovvio. Meno persone hanno privilegi di root in un sistema, meno persone conoscono la combinazione di una cassaforte, o hanno l'autorità di firmare assegni, più sicuro sarà il sistema.

2. Assicurarsi che le persone fidate siano davvero degne di fiducia. Questa è l'idea che sta alla base dei background check, dei test con le macchine della verità, del profiling della personalità, del proibire ai detenuti determinati lavori, della no-fly list della TSA, e così via; ed è anche l'idea alla base della stipulazione di polizze che assicurino l'azienda nel caso in cui queste persone non si rivelino degne di fiducia.

3. Limitare il quantitativo di fiducia di ogni persona. Questa è la divisione in compartimenti; qui l'idea è limitare l'entità dei danni che una certa persona può fare in caso si riveli indegna di fiducia. Seguendo questo concetto, ai dipendenti vengono date chiavi che aprono soltanto il loro ufficio, o password che sbloccano soltanto il loro account; analogamente vengono istituite policy di sicurezza atte a tenere informati solo i diretti interessati, e livelli di sicurezza distinti.

4. Affidare alle persone ambiti di fiducia che si sovrappongono. Questo è ciò che i professionisti della sicurezza chiamano difesa in profondità. È per questo che ci vogliono due persone con due chiavi distinte per lanciare missili a testata nucleare, e perché sono necessarie due firme su assegni aziendali che superano un certo valore. Stesso dicasi per i dipendenti di sportello in una banca, che hanno bisogno di autorizzazioni della direzione per effettuare transazioni di grandi somme e per la contabilità a partita doppia. È l'idea alla base di tutte quelle telecamere e guardie di sicurezza nei casinò. O del fatto che, quando andiamo al cinema, vi sia una persona che ci vende il biglietto e un'altra persona a pochi metri di distanza che lo strappa -- in questo modo è molto più difficile per un dipendente ingannare il sistema. È per questo che i dipendenti che ricoprono ruoli critici in una banca sono obbligati a prendersi tutti il medesimo periodo di ferie: così i loro sostituti hanno la possibilità di scoprire eventuali frodi.

5. Rilevare falle di fiducia dopo il fatto e denunciare i colpevoli. Alla fin fine, le quattro tecniche viste finora sono efficaci sino a un certo punto. Le persone fidate possono sabotare un sistema. Nella maggior parte dei casi si scopre la falla di sicurezza dopo il fatto e si punisce il responsabile attraverso il sistema legale: pubblicamente, in modo da causare un effetto deterrente e aumentare il livello generale di sicurezza nella società. È per questo che l'auditing è così importante.

Le strategie di sicurezza che abbiamo visto non proteggono soltanto contro frodi e sabotaggi, ma anche contro il problema più comune: gli errori. Le persone fidate non sono perfette, e possono fare danni inavvertitamente. Possono commettere un errore, o possono essere indotte in errore grazie ad attacchi di ingegneria sociale.

I buoni sistemi di sicurezza si servono di svariate contromisure, che funzionano tutte insieme. Fannie Mae di sicuro limita il numero di persone che hanno la capacità di inserire script malevoli nella sua rete di computer, e certamente restringe l'accesso che ha la maggior parte di queste persone. Probabilmente l'azienda è dotata di un processo di assunzione atto a ridurre il più possibile le probabilità che individui malevoli possano lavorare a Fannie Mae. E ovviamente non è dotata di una procedura di auditing grazie al quale le modifiche apportate ai server da parte di una persona siano controllate da un'altra persona -- sono certo che un tale processo sarebbe estremamente costoso. Di certo il dipartimento IT della compagnia avrebbe dovuto bloccare l'accesso di rete di Makwana immediatamente dopo il suo licenziamento, e non alla fine della giornata lavorativa.

I sistemi avranno sempre certe persone fidate in grado di sabotarli. È importante tener presente che incidenti come questo non avvengono molto frequentemente; che moltissime persone sono oneste e onorevoli. La sicurezza è progettata proprio per proteggersi dalla minoranza disonesta. E spesso piccole cose, come disabilitare un accesso subito dopo il licenziamento di un dipendente, possono essere sorprendentemente efficaci.

Questo articolo è originariamente apparso sul sito Web del Wall Street Journal.
<<http://online.wsj.com/article/SB123447990459779609.html>>

Makwana:

<<http://blogs.zdnet.com/BTL/?p=11905>>
<http://www.theregister.co.uk/2009/01/29/fannie_mae_sabotage_averted/>
<<http://blog.wired.com/27bstroke6/2009/01/fannie.html>>

La flessione economica fa aumentare la minaccia degli insider:
<<http://news.bbc.co.uk/1/hi/technology/7875904.stm>>

Dipendenti di ospedali accedono illegalmente a informazioni sui pazienti:
<http://www.schneier.com/blog/archives/2007/10/27_suspended_fo.html>

Le vulnerabilità nelle macchine per il voto elettronico:

<http://www.schneier.com/blog/archives/2006/11/voting_technolo.html>
<<http://www.nytimes.com/2008/01/06/magazine/06Vote-t.html>>
<<http://www.schneier.com/essay-101.html>>
<<http://freedom-to-tinker.com/blog/dwallach/vendor-misinformation-e-voting-world>>
oppure <<http://tinyurl.com/5c7kxn>>
<http://www.schneier.com/blog/archives/2008/08/diebold_finally.html>
<<http://blog.wired.com/27bstroke6/2009/01/diebold-audit-l.html>>
<<http://www.schneier.com/essay-068.html>>
<http://www.crypto.com/blog/ohio_voting/>

<http://www.huffingtonpost.com/kirsten-anderson/an-interview-with-david-w_b_64063.html>

oppure <<http://tinyurl.com/ad6rn3>>

Frode ai danni di una macchina per il gioco d'azzardo:

<http://www.reviewjournal.com/lvrj_home/1998/Jan-10-Sat-1998/news/6745681.html>

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

Mettere computer al posto delle persone:

<http://www.schneier.com/blog/archives/2008/12/comparing_the_s.html>

L'auditing:

<<http://www.schneier.com/blog/archives/2008/12/audit.html>>

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

Il Canile: Singularics

Questa è formidabile:

"I nostri progressi nella Teoria dei Numeri Primi hanno portato a un nuovo ramo della matematica chiamato Neutronica. Grazie alle funzioni neutroniche è possibile analizzare per la prima volta aree della matematica comunemente ritenute indefinite, come il punto in cui l'uno è diviso per zero. In sostanza abbiamo sviluppato un nuovo sistema per analizzare il punto indefinito alla singolarità che appare attraverso la matematica più elevata.

"Questa nuova tecnica di analisi ci ha fornito una conoscenza profonda del modo in cui i numeri primi vengono distribuiti attraverso i numeri interi. Secondo il sito Web della RSA, esistono più di un miliardo di istanze licenziate della crittografia a chiave pubblica RSA oggi in uso in tutto il mondo. Ognuna di queste istanze dell'algoritmo RSA basato sul numero primo può essere decifrata ora grazie all'analisi neutronica. A differenza della RSA, la Crittografia Neutronica non si basa su due grandi numeri primi, ma sulle forze neutroniche che regolano la distribuzione dei numeri primi stessi. La crittografia risultante dall'algoritmo neutronico a chiave pubblica di Singularics è teoricamente impossibile da compromettere".

Uno pensa che chiunque affermi di essere in grado di decifrare RSA alle lunghezze di chiave attualmente in uso potrebbe, che so, dimostrarlo almeno una volta. Altrimenti tutto questo può essere tranquillamente ignorato ed etichettato come ciarlataneria.

Il fondatore e CTO di Singularics sostiene inoltre di aver provato l'Ipotesi di Riemann, se avete voglia di sorbirvi il documento di 63 pagine.

<<http://www.singularics.com/products/encryption/>>

Snake oil:

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

La 'prova' dell'Ipotesi di Riemann:

<<http://www.singularics.com/science/mathematics/OnNeutronicFunctions.pdf>>

oppure <<http://tinyurl.com/agmoy9>>

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

Tre aneddoti di sicurezza dal mondo degli insetti

Le nottue della barbabietola reagiscono al suono di una vespa di passaggio immobilizzandosi dove si trovano, o anche lasciandosi cadere dalla pianta. Purtroppo non sono abbastanza intelligenti per distinguere il suono di aerei nemici (le vespe predatrici) da quello di innocui aerei commerciali (le api); reagiscono nella stessa maniera a entrambi i suoni. Così, per produrre il nettare per le api, non solo le piante vengono impollinate, ma guadagnano anche una certa protezione contro le nottue.

Il piccolo coleottero dell'alveare vive entrando negli alveari per rubare i favi e il miele. Si dirigono verso gli alveari rilevando i feromoni di allarme delle api stesse. Inoltre lasciano una scia di un lievito che fermenta il polline e rilascia sostanze chimiche che imitano i feromoni di allarme, e che attraggono a loro volta altri coleotteri che producono altro fermento. Alla fine le api sono costrette ad abbandonare l'alveare, lasciando che i coleotteri e il fermento finiscano il polline e il miele.

Il bruco della farfalla azzurra (Maculinea alcon) riesce a farsi nutrire dalle formiche falsificando un dato biometrico: i suoni prodotti dalla formica regina.

<http://scienceblogs.com/notrocketscience/2008/12/buzzing_bees_scare_caterpillars_away_from_plants.php>

oppure <<http://tinyurl.com/b2fp7m>>

<http://scienceblogs.com/notrocketscience/2009/01/beetle_and_yeast_team_up_against_bees.php>

oppure <<http://tinyurl.com/96kdea>>

<http://scienceblogs.com/notrocketscience/2009/02/butterflies_scrounge_off_ants_by_mimicking_the_music_of_quees.php>

oppure <<http://tinyurl.com/cxu8cm>>

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

La gentilezza degli sconosciuti

Quando ero piccolo, ai bambini di solito si insegnava a "non parlare agli sconosciuti". Ci dicevano che gli sconosciuti possono essere pericolosi, per cui è meglio evitarli.

Eppure la maggioranza delle persone è onesta, gentile e generosa, specialmente quando qualcuno ha bisogno di aiuto. Se un bambino piccolo è nei guai, la cosa più intelligente che può fare è cercare uno sconosciuto dall'aspetto gentile e parlargli.

Questi due consigli sembrerebbero contraddirsi a vicenda, ma in realtà non è così. La differenza è che nel secondo caso è il bambino a scegliere lo sconosciuto a cui rivolgere la parola. Dato che la stragrande maggioranza delle persone è disposta ad aiutare, è assai probabile che il bambino troverà aiuto scegliendo un estraneo qualsiasi. Ma se è lo sconosciuto ad avvicinarsi a un bambino e gli parla, non si tratta di una scelta casuale. È più probabile (ma non necessariamente probabile) che quello sconosciuto non abbia le migliori intenzioni.

Come specie, abbiamo la tendenza ad aiutarci e, sorprendentemente, moltissima della nostra sicurezza e incolumità deriva dalla gentilezza degli sconosciuti. Durante calamità quali inondazioni, terremoti, uragani, crolli di ponti. In periodi di sciagure personali. E persino nella quotidianità.

Se vi trovate seduti in un caffè a lavorare con il vostro portatile e avete bisogno di alzarvi un minuto, chiedete alla persona seduta vicino a voi di tener d'occhio i vostri effetti personali. È estremamente improbabile che vi ruberà qualcosa. Se non vi fidate, chiedete alle tre persone sedute accanto a voi. Quei tre sconosciuti non si conoscono fra loro, e non solo faranno la guardia alle vostre cose, ma vigileranno affinché nessuno di loro rubi qualcosa.

Anche in questo caso il consiglio funziona perché siete voi a scegliere le persone. Se invece siete in un caffè e tre estranei si avvicinano e si offrono di custodirvi il portatile mentre andate alla toilette, è meglio non accettare la proposta. Le probabilità che siano tre persone oneste sono molto più scarse.

Anche alcuni sistemi informatici si affidano alla gentilezza degli sconosciuti. Internet funziona perché i nodi si inoltrano benevolmente i pacchetti a vicenda senza alcuna ricompensa da parte del mittente o del destinatario di quei pacchetti. Wikipedia funziona perché degli sconosciuti sono disposti a scrivere per, e a correggere, un'enciclopedia -- senza alcuna ricompensa.

Il filtro di spam collaborativo è un altro esempio. In sostanza, una volta che qualcuno nota che una certa email è spam, la contrassegna, e tutti gli altri nella rete vengono avvertiti del fatto che sia spam. Segnalare l'email è un atto completamente altruistico: la persona che lo compie non riceve alcun vantaggio. Ma ne trae beneficio quando gli altri fanno lo stesso per altre email.

Tor è un sistema per navigare il Web in maniera anonima. I dettagli sono complicati, ma in sostanza una rete di server Tor si passano il traffico Web a vicenda in un modo che rende anonima l'origine del traffico. Immaginatelo come un grande gioco della conchiglia. Come navigatore del Web, io metto la mia richiesta Web dentro una conchiglia e la invio a un server Tor qualsiasi. Quel server sa chi sono ma non che cosa sto facendo. Quindi passa la conchiglia a un altro server Tor, che la passa a un terzo server Tor. Quel terzo server -- che sa che cosa sto facendo ma non chi sono -- processa la richiesta Web. Quando la pagina Web viene restituita a quel terzo server, il processo viene invertito e io ricevo la pagina Web richiesta. Assumendo che un numero

sufficiente di navigatori del Web stia inviando un quantitativo sufficiente di 'conchiglie' all'interno del sistema, anche se qualcuno si mette in ascolto sull'intera rete non riuscirà a capire che cosa sto facendo.

È un sistema molto ingegnoso, e protegge molte persone, fra cui giornalisti, attivisti per i diritti umani, informatori, e persone comuni che vivono sotto regimi oppressivi in ogni parte del mondo. Ma funziona soltanto grazie alla gentilezza degli sconosciuti. Nessuno riceve un beneficio dall'essere un server Tor: inoltrare i pacchetti di altri utenti consuma banda. È molto più efficiente essere un client Tor e sfruttare le capacità d'inoltro messe a disposizione dagli altri. Ma se non vi fossero dei server Tor, allora non esisterebbe la rete Tor. Tor funziona perché vi sono persone disposte ad assumersi il ruolo di server, senza alcun vantaggio diretto.

I club per gli alibi funzionano in maniera piuttosto simile. Si possono trovare su Internet, e sono gruppi slegati di persone disposte ad aiutarsi vicendevolmente creandosi alibi. Iscrivetevi e siete dentro. Potete chiedere a qualcuno di fingersi di essere il vostro medico e chiamare il vostro capo. O magari vi serve qualcuno che finga di essere il vostro capo e che chiami vostro marito o vostra moglie a casa. O magari vi serve qualcuno che finga di essere vostro marito o vostra moglie e che telefoni al vostro capo. Qualsiasi cosa vogliate, ne fate richiesta e qualcuno si offrirà volontario. Dato che il complice è uno sconosciuto senza nome, è in effetti un metodo più sicuro che non chiedere ad un amico di partecipare al vostro stratagemma.

Questi sistemi comportano dei rischi. Mercanti e altre persone guidati da scopi personali cercano di manipolare le voci della Wikipedia per adattarle ai propri interessi. Le agenzie di intelligence possono (e quasi certamente lo hanno fatto) fingersi server Tor per intercettare meglio il traffico. E un 'benefattore' potrebbe entrare in un club per gli alibi con l'unico obiettivo di esporre altri membri. Ma nella maggior parte dei casi gli sconosciuti sono disposti ad aiutarsi l'un l'altro, e i sistemi che si appoggiano a questo tipo di gentilezza funzionano molto bene su Internet.

Questo articolo è originariamente apparso sul sito Web del Wall Street Journal.
<<http://online.wsj.com/article/SB123567809587886053.html>>

Tor:
<<http://www.torproject.org/torusers.html.en>>
<<http://www.torproject.org>>

I club per gli alibi:
<<http://www.nytimes.com/2004/06/26/technology/26ALIB.html?hp>>
<<http://www.alibinetwork.com/index.jsp>>

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

Nuova frode su eBay

Ecco una frode davvero brillante, che sfrutta i ritardi di eBay, PayPal e della spedizione UPS.

“L’acquirente ha definito l’oggetto ‘distrutto’ e ha richiesto e ottenuto un risarcimento da PayPal. Quando l’acquirente ha rispedito l’oggetto e Chad ha aperto il pacco, in realtà non vi era nulla fuori posto, solo che il truffatore aveva rimosso la memoria, il processore e il disco rigido. Ora Chad ha perso 500 dollari e gli rimane il guscio di un computer. E dato che l’oggetto è stato classificato come ‘ricevuto’, PayPal non farà nulla”.

Molto astuto. Il venditore ha accettato la restituzione di UPS dopo un’ispezione visiva, quindi UPS ha considerato chiusa la faccenda. PayPal ed eBay hanno entrambi considerato chiuso il caso. Se la cifra fosse stata abbastanza elevata, il venditore avrebbe potuto sporgere denuncia, ma come avrebbe potuto provare che il computer funzionava quando lo ha venduto?

A me sembra che l’unica maniera per risolvere questo problema è che PayPal non processi alcun rimborso prima che il venditore confermi che la merce restituita sia la stessa che egli aveva precedentemente inviato. Certo, poi il venditore potrebbe commettere una truffa simile, ma i venditori (specie i venditori professionali) hanno una reputazione da difendere.

<<http://consumerist.com/5159479/ebay-scammer-says-pc-destroyed-in-mail-takes-500-sends-back-destroyed-pc-minus-parts>>
oppure <<http://tinyurl.com/czj2bu>>

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

Le news su Schneier

Schneier parlerà al MinneWebCon il 6 aprile a Minneapolis.
<<http://minnewebcon.umn.edu/>>

Schneier parlerà al 3rd Annual Asia-Pacific Programme for Senior National Security Officers (APPSNO) il 14 aprile a Singapore.
<http://www.rsis.edu.sg/cens/events/upcoming_events.html>

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

Sicurezza IT: incolpare la vittima

Dare la colpa alla vittima è una cosa piuttosto comune nel mondo IT: è colpa degli utenti perché non applicano le patch ai loro sistemi, perché scelgono password inefficaci, perché si fanno ingannare dagli attacchi di phishing, e così via. Ma malgrado gli utenti siano, e continueranno a essere, una delle maggiori cause di problemi di sicurezza, concentrarsi su di essi è un modo di pensare che non aiuta molto.

Le persone, regolarmente, non fanno cose che dovrebbero fare: cambiare l'olio della macchina, andare dal dentista, sostituire le batterie nei loro rilevatori di fumo. Perché? Perché imparano dall'esperienza. Se qualcosa procura un danno immediato -- toccare una stufa ardente o accarezzare una tigre -- le persone imparano in fretta che è meglio non farlo. Ma se si salta un cambio dell'olio, se si ignora la patch di un computer, se si sceglie una password debole, non è che importi molto. Senza feedback non c'è apprendimento.

Abbiamo cercato di risolvere la questione in vari modi. Diamo alle persone delle regole di massima: cambio dell'olio ogni 5.000 chilometri; linee guida per impostare password sicure. Oppure inviamo delle notifiche: gli allarmi antincendio emettono dei beep ripetuti, i dentisti inviano delle cartoline, Google avverte se stiamo per visitare un sito che potrebbe contenere malware. Ma, anche in questi casi, gli effetti che derivano dall'ignorare questi segnali in genere non vengono avvertiti immediatamente.

Tutto ciò fa in modo che la sicurezza sia soprattutto un ostacolo per l'utente. Ed è un intralcio ricorrente: qualcosa che interferisce con il normale flusso operativo dell'utente. È la natura umana, insita nelle nostre capacità di ragionamento, che rimuove gli ostacoli ricorrenti. Pertanto, se le conseguenze di aver ignorato o aggirato la sicurezza non sono ovvie, allora le persone continueranno ad aggirarla naturalmente.

Questo è il problema dell'User Account Control (UAC) di Microsoft. Introdotto in Vista, il concetto è quello di aumentare la sicurezza riducendo i privilegi delle applicazioni quando sono attive. Ma gli avvisi di sicurezza appaiono troppo frequentemente, ed è assai raro che vi siano effetti negativi se vengono ignorati. Quindi gli utenti li ignorano.

Ciò non significa che educare l'utente sia inutile. Al contrario, l'educazione dell'utente è una parte importante di qualunque programma di sicurezza aziendale. E a casa, più gli utenti comprendono le minacce di sicurezza e le tattiche degli hacker, più sicuri tenderanno a essere i loro sistemi. Ma dovremmo anche riconoscere i limiti dell'educazione.

La soluzione è quella di progettare meglio dei sistemi di sicurezza che partano dal presupposto di trovarsi di fronte degli utenti privi di educazione sulla sicurezza, così da evitare che modifichino impostazioni di sicurezza che li lascerebbero esposti a rischi eccessivi; o, ancora meglio, che escludano del tutto gli utenti da questioni di sicurezza.

Per esempio, tutti sappiamo che i backup sono una buona cosa. Ma se ci dimentichiamo di fare il backup questa settimana, non succederà nulla di tremendo. E se ci dimentichiamo di fare il backup più volte, continuerà a non succedere nulla di tremendo. Per cui, malgrado le nostre conoscenze sull'utilità dei backup, iniziamo a pensare che non siano poi così importanti. Apple ha trovato la soluzione giusta con Time Machine, la sua utility di backup. La si installa, si collega un disco rigido esterno, e il backup viene eseguito automaticamente, per prevenire guasti all'hardware ed errori umani. È più facile usarlo che non usarlo.

Per parte sua, Microsoft ha fatto notevoli progressi per rendere il suo sistema operativo più sicuro, offrendo impostazioni di sicurezza di default in Windows XP e ancor più in Windows Vista per garantire che un utente ingenuo non sia privo di difese quando collega il proprio computer.

Purtroppo, incolpare l'utente può essere una buona mossa commerciale. I provider di telefonia mobile risparmiano denaro se possono addebitare i propri clienti nel caso una tessera telefonica venga rubata e utilizzata in maniera fraudolenta. Le banche inglesi risparmiano denaro incolpando gli utenti quando sono vittime della frode chip-and-pin. È un problema continuo, e alcune banche arrivano perfino ad accusare la vittima di aver organizzato la frode, malgrado esistano le prove di una frode su vasta scala perpetrata da organizzazioni criminali.

Il sistema legale deve sistemare il problema sul lato commerciale, ma i progettisti di sistemi devono lavorare sulle problematiche di ordine tecnico. Devono accettare che i sistemi di sicurezza che richiedono all'utente di fare la cosa giusta sono destinati a fallire. Dopodiché devono progettare comunque una sicurezza robusta e con capacità di recupero.

Questo articolo è originariamente apparso sul Guardian.

<<http://www.guardian.co.uk/technology/2009/mar/12/read-me-first>>

Gli utenti sono un problema:

<<http://www.informationweek.com/news/security/client/showArticle.jhtml?articleID=213002007>>

oppure <<http://tinyurl.com/ab8pux>>

<<http://www.informationweek.com/news/security/attacks/showArticle.jhtml?articleID=212700890>>

oppure <<http://tinyurl.com/b2s2ep>>

Password inefficaci:

<<http://www.schneier.com/essay-144.html>>

Scegliere delle password robuste:

<<http://www.schneier.com/essay-148.html>>

I problemi dell'UAC di Microsoft:

<<http://arstechnica.com/security/news/2008/04/vistas-uac-security-prompt-was-designed-to-annoy-you.ars>>

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

I limiti dell'educazione:

<<http://www.schneier.com/essay-139.html>>

Incolpare l'utente:

<http://www.schneier.com/blog/archives/2005/12/cell_phone_comp.html>

<<http://news.bbc.co.uk/1/hi/programmes/newsnight/7265437.stm>>

Frode chip-and-pin su vasta scala:

<<http://www.telegraph.co.uk/news/newstopics/politics/lawandorder/3173346/Chip-and-pin-scam-has-netted-millions-from-British-shoppers.html>>

oppure <<http://tinyurl.com/4xuk69>>

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

Bilanciare sicurezza e usabilità nei processi di autenticazione

Da gennaio, il worm Conficker.B si è propagato molto rapidamente in tutta Internet: ha infettato la Marina francese, degli ospedali a Sheffield, il sistema giudiziario a Houston, e milioni di computer in tutto il mondo. Uno dei modi con cui si diffonde è craccando password di amministratore di rete. Il che porta all'interrogativo più importante: perché diamine gli amministratori IT continuano a usare password facili da indovinare?

I sistemi di autenticazione computerizzati hanno due requisiti di base. Devono evitare che i malviventi accedano al nostro account, e devono permettere a noi di accedere al nostro account. Sono due presupposti ugualmente cruciali, e ogni sistema di autenticazione è un atto di bilanciamento fra i due. Una sicurezza troppo scarsa, e i malviventi entreranno fin troppo facilmente. Ma se il sistema di autenticazione è troppo complicato, restrittivo, o difficile da utilizzare, non saremo in grado (o non ci prenderemo nemmeno la briga) di usarlo.

Le password sono il sistema di autenticazione più comune, e anche un ottimo punto di partenza. Sono molto semplici da implementare e da usare, ed è per questo che sono molto diffuse. Ma con l'aumento di velocità e prestazioni dei computer, il password guessing (indovinare una password per tentativi) è diventato più facile. La maggior parte delle persone non scelgono password sufficientemente complesse da resistere ai moderni attacchi di password guessing. Conficker.B è ancor meno brillante: prova semplicemente pescando da un elenco delle 200 password più comuni.

Per contrastare il password guessing molti sistemi obbligano gli utenti a scegliere password difficili da indovinare -- che richiedono una lunghezza minima, o caratteri non alfanumerici, ecc. -- e a cambiarle più di frequente. Il primo metodo rende le password più difficili da indovinare, il secondo riduce il valore di una password indovinata. Il tutto, naturalmente, rende il sistema più fastidioso, e così gli utenti si scrivono le password su pezzi di carta o post-it che poi appiccicano sui loro monitor, oppure si dimenticano le password più frequentemente. Gli utenti più in gamba si segnano le password su un biglietto che poi infilano nel portafoglio, oppure ricorrono a un database di password sicuro come Password Safe.

Gli utenti che si dimenticano le password possono rappresentare un costo elevato: gli amministratori di sistema o i rappresentanti dei servizi di attenzione al cliente devono rispondere alle chiamate e resettare le password, pertanto alcuni sistemi sono dotati di un meccanismo di autenticazione di backup: una domanda segreta. L'idea è che se ci dimentichiamo la password, possiamo autenticarci grazie a certe informazioni personali che solo noi conosciamo. Un classico è il cognome di nostra madre da nubile, ma oggi le domande segrete sono fra le più variegatae: il professore preferito, il colore preferito, il nome della via in cui siamo cresciuti, il nome del nostro primo animale domestico, e così via. Questo potrebbe rendere il sistema più usabile, ma anche meno sicuro: le risposte possono essere molto facili da indovinare, e persone a noi vicine possono conoscerle.

Una soluzione più sofisticata e altrettanto comune è un generatore di password da usarsi una sola volta, come una chiavetta SecurID. Si tratta di un piccolo dispositivo che visualizza una password che cambia automaticamente ogni minuto. L'aggiunta di questo meccanismo viene chiamata autenticazione a due fattori, ed è molto più sicura, perché questa chiavetta -- qualcosa in nostro possesso -- viene combinata con una password -- qualcosa che conosciamo. Ma è meno usabile, perché occorre acquistare le chiavette e distribuirle a tutti gli utenti, e troppo spesso il dispositivo diventa 'qualcosa che abbiamo perso o dimenticato'. E costa denaro. Le chiavette vengono utilizzate più frequentemente in ambienti aziendali, ma anche le banche e certi universi ludici online hanno iniziato a farne uso -- a volte in maniera facoltativa, perché non piacciono alle persone.

Nella maggior parte dei casi, come funziona un sistema di autenticazione quando un utente legittimo prova a effettuare il login è molto più importante di come funziona il sistema quando è un impostore a tentare il login. Non esiste un sistema di sicurezza perfetto, ed esiste un certo livello di frode associato a questi metodi di autenticazione. Ma i casi di frode sono rari se paragonati a quante volte qualcuno cerca di effettuare il login in forma legittima. Se un determinato sistema di autenticazione lasciasse penetrare i malviventi una volta su cento, una banca potrebbe decidere di convivere con il problema, oppure tentare di risolverlo in qualche altra maniera. Ma se quello stesso sistema di autenticazione impedisse ai clienti legittimi di autenticarsi anche solo una volta su cento, la quantità di reclami sarebbe tale che il sistema non durerebbe una settimana.

Bilanciare la sicurezza e l'usabilità è arduo, e molte organizzazioni non riescono a farlo correttamente. Ma c'è un'evoluzione: le organizzazioni che hanno bisogno di rendere più rigorosa la propria sicurezza continuano a spingere metodi di autenticazione più complicati, e un numero sempre maggiore di utenti Internet sono disposti ad accettarli. E sicuramente gli amministratori IT devono guidare tale cambiamento evolutivo.

Una versione del presente articolo è stata originariamente pubblicata sul Guardian.

<<http://www.guardian.co.uk/technology/2009/feb/19/insecure-passwords-conflickerb-worm>>

oppure <<http://tinyurl.com/awd5np>>

Conficker.B:

<<http://www.crn.com/security/212902319>>

<<http://www.telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html>>

oppure <<http://tinyurl.com/bbku57>>

<<http://www.smarthealthcare.com/sheffield-conficker>>

<http://www.theregister.co.uk/2009/02/09/houston_malware_infection/>

<<http://arstechnica.com/security/news/2009/01/conficker-worm-spikes-infects-1-1-million-pcs-in-24-hours.ars>>

oppure <<http://tinyurl.com/dmvd8d>>

<http://securitywatch.eweek.com/virus_and_spyware/experts_-_conficker_usb_worm_spreading_quickly.html>

oppure <<http://tinyurl.com/bk5fs9>>

<http://voices.washingtonpost.com/securityfix/2009/01/tricky_windows_worm_wallops_mi.html>

oppure <<http://tinyurl.com/8e8fbg>>
<http://bt.counterpane.com/Risk_Assessment_W32.Conficker_Worm_Update2.pdf>
oppure <<http://tinyurl.com/detvm5>>
<<http://www.microsoft.com/security/portal/Entry.aspx?Name=Worm:Win32/Conficker.B>>
oppure <<http://tinyurl.com/9vpbxs>>
<<http://www.sophos.com/blogs/gc/g/2009/01/16/passwords-conficker-worm/>>

Indovinare le password:

<<http://www.schneier.com/essay-246.html>>
<<http://www.schneier.com/essay-148.html>>

Password Safe:

<<http://www.schneier.com/passsafe.html>>

Problemi di sicurezza legati alle 'domande segrete':

<http://www.schneier.com/blog/archives/2005/02/the_curse_of_th.html>

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

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>>

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

Dal 1998 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>

I commenti a CRYPTO-GRAM devono essere inviati a 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) 2009 - Bruce Schneier.