

CRYPTO-GRAM
15 dicembre 2004

Scritta da Bruce Schneier
Fondatore e CTO di Counterpane Internet Security, Inc.

Edizione italiana curata da Communication Valley SpA

E-mail: schneier@counterpane.com

Web: <<http://www.schneier.com>> oppure <<http://www.counterpane.com>>

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

Crypto- Gram in versione originale è anche consultabile in formato RSS:
<<http://www.schneier.com/crypto-gram-rss.xml>>

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

** **

In questo numero:

Il profiling basato sull'analisi comportamentale (Behavioral Assessment Profiling)

Le ristampe di Crypto- Gram

Google Desktop Search

News

Note di sicurezza da ogni dove: Gli interrogatori della Sicurezza dell'aeroporto di Israele

Le News di Counterpane

Il Canile: Internet Security Foundation

Kafka e la Persona Digitale

Lo EPIC (Electronic Privacy Information Center)

Per un uso sicuro del personal computer

Commenti dei lettori

** **

Il profiling basato sull'analisi comportamentale (Behavioral Assessment Profiling)

<http://www.schneier.com/blog/archives/2004/11/profile_hinky.html>

Il 14 dicembre 1999, Ahmed Ressam tentò di penetrare negli Stati Uniti dal Canada a Port Angeles, Washington. Aveva una valigetta esplosiva nel baule della sua automobile. Un ufficiale doganale statunitense, Diana Dean, lo interrogò alla frontiera. Era agitato, sudato, e nervoso. Evitava lo sguardo del suo interlocutore. Usando le parole di Dean, “aveva un'aria strana”. L'auto di Ressam è stata poi perquisita, e lui arrestato.

Non è stato un dettaglio particolare a insospettire Dean, ma tutto ciò che racchiude la frase “aveva un'aria strana”. Ed ha funzionato. Se non è stata piazzata una bomba nel Los Angeles International Airport intorno al Natale 1999, è grazie all'intuito e all'attenzione di un ufficiale di sicurezza addestrato e preparato.

Questo è il profiling basato sulla cosiddetta “analisi comportamentale”. È ciò che gli agenti doganali fanno sempre alle frontiere. È ciò che la polizia israeliana fa per proteggere aerei e aeroporti in Israele. Ed è parte di un nuovo programma al Logan Airport di Boston, negli Stati Uniti. Il profiling comportamentale è pericoloso perché è facile abusarne, ma è anche la cosa migliore che possiamo fare per migliorare la sicurezza dei passeggeri delle nostre linee aeree.

Il profiling comportamentale è ben diverso dal profiling computerizzato dei passeggeri. Quest'ultimo viene utilizzato da anni. È un sistema segreto, ed è un grosso pasticcio. A volte le compagnie aeree hanno deciso chi avrebbe subito un secondo controllo, basandosi ad esempio sul metodo di acquisto del biglietto, o se un passeggero fosse un frequent flyer o meno, o se il nome del passeggero fosse simile a uno di quelli compresi nelle watch list governative. CAPPS-2 sarebbe seguito di lì a poco, analizzando le persone basandosi su database governativi e commerciali e assegnando di conseguenza un “punteggio rischio”. Tale sistema è stato accantonato a seguito delle proteste dell'opinione pubblica, ma un altro sistema di profiling chiamato Secure Flight debutterà il prossimo anno. Ancora una volta, i dettagli rimangono segreti.

Il problema del profiling computerizzato dei passeggeri, semplicemente, è che non funziona. I terroristi non corrispondono a un profilo preciso e non possono essere individuati e separati dalla folla grazie a un computer. I terroristi possono essere europei, asiatici, africani, ispanici, mediorientali, di sesso maschile e femminile, giovani e vecchi. Richard Reid, lo “shoe bomber”, era inglese di padre giamaicano. Jose Padilla, arrestato a Chicago nel 2002 in quanto sospettato di aver fabbricato un ordigno esplosivo artigianale, era latino-americano. Timothy McVeigh era un americano di razza bianca. Stesso dicasi per Unabomber, che un tempo insegnava matematica all'università di Berkeley, California. I ceceni che hanno fatto saltare due aerei russi lo scorso agosto erano donne. Recenti comunicati affermano che Al Qaeda stia reclutando dei cittadini europei per scagliare nuovi attacchi agli Stati Uniti.

I terroristi possono acquistare biglietti aerei, sia di sola andata che di andata e ritorno, in contanti o con carta di credito. Mohamed Atta, il leader del complotto dell'11 settembre, era un frequent flyer con “carta oro”. Esistono gruppi di persone straordinariamente diversificati, e un qualsiasi sistema computerizzato di profiling non farà altro che rendere la vita più facile a chi non corrisponde a un certo profilo.

Il profiling basato sull'analisi comportamentale è molto diverso. Non bada a tutte quelle caratteristiche superficiali di profiling e punta dritto alla persona. La polizia di stato è addestrata a questo tipo di controlli per individuare comportamenti sospetti quali atteggiamenti furtivi o abnorme ansietà. Il programma in vigore al Logan Airport ha già catturato 20 persone che si trovavano nel paese illegalmente o che avevano mandati di cattura pendenti delle specie più varie.

Agli inizi di questo mese, la ACLU del Massachusetts ha intentato una causa mettendo in questione la costituzionalità del profiling basato sull'analisi comportamentale. Ma la causa non ha molte probabilità di successo; il principio del “tacito assenso”, usato per sostenere la legalità dei controlli su passeggeri e bagagli, verrà certamente applicato anche in questo caso.

Ma l'ACLU è in torto. Il profiling basato sull'analisi comportamentale non è il problema. Il problema è l'abuso di tale metodo di profiling, e l'ACLU ha identificato correttamente in quali casi può essere uno sbaglio. Se la polizia si limita ad un profiling ingenuo basato su razza, etnia, età e sesso (caratteristiche irrilevanti ai fini della sicurezza), non faranno un lavoro molto migliore di un computer. In questo modo la polizia dovrà affrontare l'accusa di aver infastidito la gente per il reato di “Arabo in volo”, piuttosto che “Negro alla guida”. Le loro azioni faranno aumentare le tensioni razziali e li renderanno meno inclini a individuare le vere minacce. E di conseguenza noi tutti saremo meno sicuri.

Il profiling basato sull'analisi comportamentale non è la panacea di tutti i mali, ma deve essere una parte di un sistema di sicurezza a più livelli, un sistema che includa il controllo dei bagagli dei passeggeri, un controllo degli impiegati dell'aeroporto, e controlli casuali di sicurezza. Viene messo in pratica al meglio non dalla polizia, ma da ufficiali federali addestrati all'uopo. Questi ufficiali potrebbero essere impiegati negli aeroporti, negli stadi, durante manifestazioni politiche, e in genere

<<http://www.cryptogram.it/dicembre.html#a4>> (traduzione)

Farsi beffe degli scanner di vulnerabilità:

<<http://www.schneier.com/crypto-gram-0112.html#9>>

<<http://www.cryptogram.it/dicembre.html#a9>> (traduzione)

Le votazioni e la tecnologia:

<<http://www.schneier.com/crypto-gram-0012.html#1>>

“La Sicurezza non è un Prodotto; è un Processo”:

<<http://www.schneier.com/crypto-gram-9912.html#1>>

La tecnologia Echelon:

<<http://www.schneier.com/crypto-gram-9912.html#3>>

Gli algoritmi digitali cellulari europei:

<<http://www.schneier.com/crypto-gram-9912.html#10>>

L'inutilità delle gare di cracking:

<<http://www.schneier.com/crypto-gram-9812.html#contests>>

Come riconoscere il testo in chiaro (plaintext):

<<http://www.schneier.com/crypto-gram-9812.html#plaintext>>

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

Google Desktop Search

<http://www.schneier.com/blog/archives/2004/11/desktop_google.html>

Il software Desktop Search di Google è fatto così bene che espone delle vulnerabilità del vostro computer di cui non eravate nemmeno a conoscenza.

Il mese scorso, Google ha rilasciato una versione beta di Google Desktop Search, il suo software che permette di effettuare ricerche sul proprio computer. Installandolo sul vostro PC Windows, esso crea un indice dei vostri file di dati (fra cui file di testo, fogli di calcolo, presentazioni, messaggi e-mail, pagine Web presenti nella cache e sessioni di chat) su cui poter effettuare ricerche di ogni tipo. È un'ottima idea: le capacità di ricerca di Windows sono sempre state mediocri, e Google pone un buon rimedio a tutto questo.

Però esistono anche problemi di sicurezza. Il guaio è che GDS indicizza e trova documenti che magari vorreste non fossero trovati. Per esempio, GDS effettua ricerche nella cache del vostro browser. Il che gli permette di trovare vecchie pagine Web che avete visitato, fra cui riepiloghi di operazioni di banking online, messaggi personali inviati da programmi di posta basati sul Web, e pagine Web protette da password.

GDS può anche recuperare file criptati. No, non aggira la criptatura né salva una copia della chiave. Tuttavia va a cercare nella cache di Windows, che può aggirare completamente alcuni programmi di crittografia. E se installate il programma su un computer in multiutenza, è possibile cercare documenti e pagine Web di tutti gli utenti.

GDS non fa nulla di male; indicizza e ricerca i documenti proprio come dovrebbe. Le vulnerabilità sono dovute alla struttura del sistema operativo che sta sotto e dalle sue applicazioni.

Primo, i browser Web non dovrebbero memorizzare pagine crittografate SSL o pagine con e-mail personali. E se lo fanno, dovrebbero almeno chiederne il permesso all'utente.

Secondo, un programma di crittografia che lascia copie di file decrittati nella cache è progettato male. Quei file rimangono lì, a prescindere che GDS li cerchi.

Terzo, la capacità di GDS di ricercare file e pagine Web di più utenti su un medesimo computer ha suscitato parecchie polemiche e commenti a livello stampa quando fu scoperta. Ma questo è decisamente un non-problema, perché per farlo occorre essere amministratori del computer, e ciò dà comunque accesso ai file di tutti.

Alcuni incolpano Google per tali problemi e suggeriscono, a torto, che Google vi ponga rimedio. Che succederebbe se Google modificasse GDS per fare in modo che non visualizzi informazioni private? I problemi sottesi rimarrebbero: le pagine Web private resterebbero comunque nella cache del browser; il programma di crittografia continuerebbe a lasciare copie di file di testo in chiaro nella cache del sistema operativo e l'amministratore di sistema potrebbe ugualmente spiare i computer degli altri utenti a cui ha accesso. L'unica cosa da cambiare è che queste vulnerabilità rimarrebbero ancora una volta nascoste all'utente comune.

Alla fine, tutto questo non può che danneggiare la sicurezza.

GDS è molto buono per le ricerche. Talmente buono che espone delle vulnerabilità del vostro computer di cui non eravate nemmeno a conoscenza. Ora che ne siete a conoscenza, fate in modo che siano i produttori dei software a sistemarle. Non prendetevela con l'ambasciatore, che non porta pena.

Interventi su GDS:

<http://www.eweek.com/print_article2/0,2533,a=137394,00.asp>

<<http://www.pcmag.com/article2/0,1759,1710823,00.asp>>

Una versione di questo articolo è apparsa in precedenza su eWeek:

<<http://www.eweek.com/article2/0,1759,1730748,00.asp>>

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

News

Amtrak sta ora effettuando controlli casuali sui documenti d'identità.

<<http://www.cnn.com/2004/TRAVEL/11/18/amtrak.id.checks.ap/index.html>>

Ho già trattato in precedenza di cose come questa. È il genere di procedimento che non ci rende più sicuri, che spreca il nostro tempo e il denaro di Amtrak.

<<http://www.schneier.com/essay-008.html>>

Una banca neozelandese sta implementando l'autenticazione a due fattori mediante telefono cellulare. Funziona ottimamente se tutti i vostri clienti hanno un cellulare.

<<http://www.smh.com.au/news/Breaking/NZ-bank-adds-security-online/2004/11/08/1099781306318.html>> oppure

<<http://makeashorterlink.com/?M1172260A>>

Un furto d'auto impressionante:

<<http://www.bloomberg.com/apps/news?pid=10000085&sid=aRaEXeRubjHc>>

Vi sono due tipi di ladri, che siano ladri d'auto o meno. 1) ladri che vogliono un'automobile qualsiasi e 2) ladri che vogliono un'automobile in particolare. Contro il primo tipo basta qualsiasi misura di sicurezza che renda la propria auto più difficile da rubare rispetto a quella accanto. Contro il secondo tipo, nemmeno un sistema di tracciamento GPS può essere sufficiente.

Bletchey Park quest'anno ospita una conferenza sulla sicurezza:

<<http://www.bletchleypark.org.uk/page.cfm?PageID=294&EventID=94>>

Lycos sta divulgando un salvaschermo che sovraccarica i siti di spam:

<http://www.theregister.co.uk/2004/11/26/lycos_europe_spam_blitz/print.html>

oppure <<http://makeashorterlink.com/?Q2273260A>>

<<http://news.bbc.co.uk/2/hi/technology/4051553.stm>>

<http://news.com.com/Lycos+Europes+zombie+campaign+downs+two+sites/2100-7349_3-5474963.html> oppure <<http://makeashorterlink.com/?G5371260A>>

Ho parlato di questo in precedenza, ed è una cattiva idea:

<<http://www.schneier.com/crypto-gram-0212.html#1>>

Assennate riflessioni sulla sicurezza provenienti dalla Nuova Zelanda:

<<http://www.nzherald.co.nz/index.cfm?ObjectID=3600794>>

Una storia illustrata delle casseforti e dell'arte di scassarle:

<http://www.timhunkin.com/94_illegal_engineering.htm>

Un documento del 1959 che parla di un generatore hardware di numeri casuali collegato a un computer.

<http://phk.freebsd.dk/rc3600/DASK_rng.pdf>

La Sovrintendenza all'Informazione e alla privacy della Provincia del British Columbia, in Canada, ha pubblicato un rapporto intitolato "Privacy and the USA Patriot Act - Implications for British Columbia Public Sector Outsourcing." [La privacy e il Patriot Act USA - Implicazioni sull'outsourcing nel settore pubblico del British Columbia].

<http://www.oipc.bc.ca/sector_public/usa_patriot_act/pdfs/report/privacy-final.pdf>

oppure

<<http://makeashorterlink.com/?F3472260A>>

Il gruppo di standard ANSI X.9 è alla ricerca di un nuovo algoritmo di key-wrapping. Vi sono parecchi candidati, e ora si fa necessaria una buona crittanalisi:

<<http://eprint.iacr.org/2004/340/>>

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

Note di sicurezza da ogni dove: gli interrogatori della sicurezza dell'aeroporto di Israele

http://www.schneier.com/blog/archives/2004/12/security_notes.html

Sia in "Secrets and Lies" che in "Beyond Fear", parlo della fondamentale differenza fra aggressori e difensori: la capacità di concentrare le risorse. Il difensore deve difendersi da tutti gli attacchi possibili, mentre l'aggressore può concentrare le sue forze su un tipo specifico d'attacco. Questa regola è alla base di moltissime situazioni di sicurezza, e può essere vista in atto molto chiaramente nella lotta antiterrorismo. Un paese è nella posizione dell'interno, deve difendersi contro ogni possibile attacco terroristico: terrorismo aereo, ordigni chimici, minacce nei porti di mare, minacce attraverso le poste, pazzi solitari con armi automatiche, assassini, eccetera eccetera. Al terrorista basta trovare un punto debole nelle difese, e sfruttarlo. Questa concentrazione, di contro alla dispersione delle risorse, è il motivo per cui il compito del difensore è ben più arduo di quello dell'aggressore.

Questo stesso principio è di guida negli interrogatori di sicurezza condotti all'aeroporto Ben Gurion in Israele. In questo esempio, l'aggressore è l'ufficiale di controllo sicurezza e il difensore è il terrorista. (È importante ricordare che "aggressore" e "difensore" non sono etichette morali, ma tattiche. A volte i difensori sono i "buoni" e gli aggressori i "cattivi". In questo caso, il cattivo sta cercando di difendere la sua storia di copertura contro il buono che la sta attaccando, mettendo in discussione).

La sicurezza nell'aeroporto è sorprendentemente forte, e comprende una potenziale, lunga "intervista" condotta da un ufficiale di sicurezza addestrato. L'ufficiale fa domande a ogni passeggero, cercando di capire se il tal passeggero può essere un rischio per la sicurezza. Però, invece di fare domande diverse fra loro (dove vive? qual è il suo lavoro? dov'è nato?), l'ufficiale chiede cose che seguono un percorso, una storia: "Dove si sta recando? Chi conosce laggiù? Come ha incontrato questa persona? Che cosa stava facendo laggiù?" e così via.

Vedete la capacità di concentrare risorse? Il difensore (il terrorista che cerca di introdursi a bordo dell'aereo) ha bisogno di una storia di copertura sufficientemente ampia e articolata per essere in grado di rispondere a qualsiasi tipo di interrogatorio. Per cui potrebbe memorizzare le risposte utili per centinaia di domande. L'aggressore (l'ufficiale di sicurezza) potrebbe fare domande diversificate a raffica, ma invece concentra il suo interrogatorio su una linea di percorso precisa. L'idea è che a un certo punto il difensore raggiungerà la fine della sua storia, e a quel punto l'aggressore noterà i piccoli cambiamenti del difensore mentre comincia a inventare risposte.

** **

Le News di Counterpane

Non ho interventi in pubblico da qui al 15 gennaio. I miei auguri di Buone Feste a tutti voi.

Schneier è stato intervistato sulla sorveglianza generale da TechWeb:
<<http://www.techweb.com/rss/54200987>>

Counterpane ha suscitato parecchio interesse in conformità con la sezione relativa alla protezione e privacy dei dati nella disposizione Sarbanes-Oxley della Security and Exchange Commission statunitense. Visitate il sito Web di Counterpane per una lettura del libro bianco sull'argomento:
<<http://www.counterpane.com/soxwhitepaper>>

** **

Il Canile: Internet Security Foundation

<http://www.schneier.com/blog/archives/2004/12/the_doghouse_in.html>

Questa organizzazione vuole vendere il proprio strumento per visualizzare le password nei campi di testo "nascoste" da Windows mediante asterischi. Dichiarano come questo sia "un madornale buco di sicurezza di Microsoft Windows" e "un grave rischio per la sicurezza". La loro pagina Web è ricca di FUD ["Fear, Uncertainty, Doubt", ovvero disinformazione finalizzata a gettare discredito sulla concorrenza instillando nell'utente paura, incertezza e dubbio riguardo ai prodotti della concorrenza. N.d.T.] e mette in guardia sul fatto che criminali e terroristi possono facilmente ripulirvi il vostro conto in banca a causa di questo problema.

Ovviamente il problema non è dovuto al fatto che gli utenti inseriscano password nei propri computer. Il problema è che i programmi non conservano le password in maniera sicura. Il problema è che i programmi inoltrano le password in chiaro. Il problema è che gli utenti scelgono pessime password, e le conservano in maniera poco sicura. Il problema è che le applicazioni finanziarie, per quanto riguarda la sicurezza, si affidano ancora sulle password e non sull'autenticazione a due fattori.

Ma la "Internet Security Foundation" sta cercando di fare più rumore possibile. Hanno persino preparato una letteraccia a Bill Gates che potete firmare (l'ultima volta che ho guardato, i firmatari erano 36). Non ho ben capito quale sia la loro angolazione, ma non mi piace.

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

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

Kafka e la Persona Digitale

<http://www.schneier.com/blog/archives/2004/12/the_digital_per.html>

La scorsa settimana ho soggiornato all'hotel St. Regis a Washington DC. Era la mia prima visita, e la direzione mi ha dato un questionario in cui mi venivano chieste cose come la mia data di nascita, quella di mia moglie e il suo nome da nubile, il nostro anniversario, e quali fossero i miei frutti, dolci e bevande preferiti. Lo scopo era chiaro: l'albergo voleva essere in grado di fornirmi un servizio più personalizzato alla mia eventuale visita successiva. E tale scopo mi vedeva concorde: mi avrebbe fatto piacere un servizio personalizzato. Tuttavia mi trovavo a disagio nel compilare quel modulo.

Non che le informazioni fossero particolarmente riservate. Della mia data di nascita, del mio anniversario di nozze, dei miei gusti in fatto di cibo, non faccio segreto. Molte di tali informazioni credo siano addirittura in giro per il Web. La segretezza non era il problema.

Il problema era il controllo. negli Stati Uniti, le informazioni di una persona sono proprietà di chi le raccoglie, non della persona stessa. Vi sono specifiche eccezioni previste dalla legge, ma sono rarissime. Non esistono leggi sulla protezione dei dati, come nell'Unione Europea. Non vi sono Sovrintendenze alla Privacy, come in Canada. La legge sulla privacy negli Stati Uniti è in gran parte basata sulla segretezza: se certe informazioni non sono segrete, allora potete farci ben poco per evitarne la divulgazione.

Come conseguenza, esistono enormi database zeppi di informazioni personali. Questi database appartengono ad aziende di marketing, compagnie di credito, e al governo. Amazon sa quali libri acquistiamo. Il nostro supermarket sa che cibo mangiamo. Le compagnie di carte di credito sanno molte cose sulle nostre abitudini negli acquisti. Le compagnie di credito conoscono la nostra storia finanziaria, e quel che non sanno è contenuto negli archivi delle banche. I registri governativi contengono i nostri codici di previdenza sociale, anni di nascita, indirizzi, nome da nubile delle nostre madri, e tutta una serie di altri dati. Molti registri della motorizzazione contengono fototessere digitali.

Tutte queste informazioni vengono combinate, indicizzate, correlate, e vengono utilizzate per ogni genere di cose. Le campagne di marketing finalizzate sono solo la punta dell'iceberg. Questi dati vengono usati da potenziali datori di lavoro per giudicare la nostra idoneità come impiegati, da potenziali padroni di casa per determinare la nostra idoneità come inquilini, e dal governo per determinare la nostra probabilità di essere terroristi.

Alcuni centri commerciali stanno iniziando ad usare i nostri dati per stabilire se siamo "clienti desiderabili" o meno. Se certi clienti sfruttano troppe offerte speciali o restituiscono la merce con troppa frequenza, potrebbero essere etichettati come "cattivi" clienti e venire trattati diversamente dai clienti "buoni".

E con allarmante frequenza i nostri dati vengono abusati da ladri d'identità. Le organizzazioni che raccolgono i nostri dati non si danno molta pena per metterli al sicuro. Perciò il furto d'identità è un problema dove le vittime, i singoli individui, non sono nella posizione di migliorare la sicurezza, e coloro che sono in tale posizione non sono vittime del problema.

Per molti cittadini americani, la fine dell'anno è un'occasione per contributi caritatevoli (i motivi sono essenzialmente fiscali). Ci sono indubbiamente molte valide cause da sostenere in tutto il mondo, ad ogni modo vorrei consigliare di devolvere qualcosa anche allo EPIC.

Dalla sua fondazione, dieci anni fa, EPIC ha lavorato per proteggere la privacy, la libertà di espressione, i valori democratici, e per sostenere la voce del pubblico in decisioni che riguardano il futuro di Internet. EPIC mantiene uno dei siti Web più esaustivi sulla privacy, e sulle problematiche legate alla libertà di parola, di tutta Internet. Contestano in sede processuale il Freedom of Information Act, il Primo Emendamento e i casi di privacy. Pubblicano libri sull'open government e la privacy. Educano gli studenti di legge in merito a Internet e all'interesse pubblico. Testimoniano con frequenza davanti al Congresso in merito a problematiche emergenti sulle libertà civili. Offrono un elenco esauriente di risorse sulla privacy e una guida a strumenti pratici per la privacy.

Vi ricordate quando divenne pubblica la notizia che JetBlue (e altre compagnie aeree) passava informazioni sui passeggeri al governo USA violando le proprie politiche sulla privacy? O quando fu rivelato che CAPPIS-II, il sistema di profiling di passeggeri delle linee aeree sarebbe stato usato per scopi non inerenti all'antiterrorismo? Fu il lavoro di EPIC legato al Freedom of Information Act a rivelare quelle notizie.

Il 15 dicembre è il 213esimo anniversario della sottoscrizione del Bill of Rights. Leggetelo un'altra volta oggi, e fate caso a come le varie leggi proteggano la sicurezza degli americani. Sono orgoglioso di essere un membro del comitato consultivo di EPIC. Sono persone che fanno un ottimo lavoro, e grazie ad esso siamo tutti molto più sicuri.

Il sito Web di EPIC:
<<http://www.epic.org/>>

Il Bill of Rights statunitense:
<http://www.archives.gov/national_archives_experience/charters/bill_of_rights.html> oppure
<<http://makeashorterlink.com/?H2576260A>>

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

Per un uso sicuro del personal computer

<http://www.schneier.com/blog/archives/2004/12/safe_personal_c.html>

Con regolarità mi viene chiesto che cosa possono fare gli utenti medi di Internet per accertarsi della loro sicurezza. La mia prima risposta in genere è "Niente. Siete fregati".

Ma non è vero, la realtà delle cose è più complicata. Siete fregati se non fate nulla per proteggervi, ma vi sono molte cose che potete fare per aumentare la vostra sicurezza in Internet.

Due anni fa ho pubblicato un elenco di consigli per la sicurezza del PC. L'idea era quella di fornire agli utenti domestici delle azioni pratiche da compiere per migliorare la sicurezza. Quel che segue è un aggiornamento di quella lista: una decina di cose che potete fare per migliorare la vostra sicurezza.

In generale: spegnete il computer quando non lo state usando, specialmente se avete una connessione Internet sempre attiva.

Sicurezza dei portatili: tenete il vostro portatile sempre con voi quando non siete a casa; trattatelo come fosse un portafogli o una borsetta. Eliminate regolarmente ogni file che non vi serve più. Stesso dicasi per i palmari. La gente tende a conservare più dati personali (fra cui password e PIN) sui palmari molto più che sui PC portatili.

Backup: fate backup regolari. Fate il backup su un hard disk, su un'unità a nastro o su CD-ROM. Vi sono molte cose da cui non potete difendervi; un backup recente vi permetterà se non altro di riprendervi dopo un attacco. Conservate almeno un set di backup in un altro luogo (ottimo luogo è una cassetta di sicurezza) e almeno un altro sul luogo di lavoro. Ricordatevi di distruggere i vecchi backup. Il modo migliore per distruggere i CD-R è quello di metterli nel microonde e impostare il forno sul massimo per cinque secondi. Potete anche spezzarli in due o buttarli in qualche trinciatrice.

Sistemi operativi: se possibile, non usate Microsoft Windows. Compratevi un Macintosh o usate Linux. Se proprio dovete usare Windows, impostate "Aggiornamento Automatico" in modo da ricevere automaticamente le patch di sicurezza. Cancellate i file "command.com" e "cmd.exe".

Applicazioni: limitate il numero di applicazioni sulla vostra macchina. Se non avete bisogno di un certo programma, non installatelo. Se non ne avete più bisogno, disinstallatelo. Come alternativa a Microsoft Office, valutate le altre suite disponibili gratuitamente. Controllate periodicamente la presenza di eventuali aggiornamenti delle applicazioni che usate e installateli. Mantenere aggiornati i propri programmi è importante, ma non è necessario perderci ore di sonno.

Browser Internet: non usate Microsoft Internet Explorer, punto. Limitate l'uso di cookie e applet a quei pochi siti che offrono servizi a voi necessari. Impostate il vostro browser in modo che cancelli regolarmente i cookie. Non assumete che un sito Web sia quel che dice di essere, a meno che non abbiate inserito voi stessi l'URL. Assicuratevi che la barra degli indirizzi mostri l'indirizzo Web esatto, non uno molto simile.

Siti Web: la presenza di SSL (Secure Socket Layer) non offre alcuna garanzia che il venditore sia degno di fiducia o che il suo database di informazioni sui clienti sia sicuro.

Pensateci due volte prima di fare business con un sito Web. Limitate i dati personali e finanziari che inviate a siti Web: non divulgate informazioni a meno che non vi sembri vantaggioso farlo. Se non volete fornire i vostri dati personali, mentite. Rifiutate invii di materiale di marketing. Se il sito Web vi offre la possibilità di non registrare le vostre informazioni per usi futuri, sfruttatela. Per gli acquisti on-line, utilizzate una carta di credito, non una carta di debito.

Password: Non riuscite più a memorizzare delle buone password, per cui non sforzatevi. Per siti Web ad alta sicurezza, come quelli delle banche, create lunghe password casuali e scrivetele. Custoditele come fossero il vostro denaro contante: mettetele nel portafoglio, ecc.

Non riutilizzate mai una password per qualcosa che per voi ha importanza. Va bene avere un'unica password per siti a bassa sicurezza, come quelli per accedere agli archivi dei quotidiani online. Presumete che tutti i PIN possano essere facilmente craccati e agite di conseguenza.

Non scrivete mai una password importante, come quella di un conto bancario, in una pagina non crittata SSL. Se la vostra banca ve lo fa fare, lamentatevi. Quando vi dicono che va bene così, non credete loro: hanno torto.

E-mail: disattivate l'e-mail HTML. Non date automaticamente per scontato che ogni e-mail che ricevete provenga dall'indirizzo nel campo "Da:".

Cancellate lo spam senza leggerlo. Non aprite messaggi con allegati, a meno che non sappiate ciò che contengono. Altrimenti, cancellateli subito. Non aprite cartoni animati, video e simili file "per farsi due risate" che amici benintenzionati vi hanno inoltrato. Ancora una volta, cancellateli subito.

Non fate mai clic su link contenuti in un messaggio e-mail a meno che non siate sicuri della bontà dell'e-mail. Copiate e incollate il link nel vostro browser invece. Non usate Outlook o Outlook Express. Se dovete usare Microsoft Office, attivate la protezione da virus macro; in Office 2000 attivate il livello di sicurezza "alto" e non fidatevi di alcun file ricevuto a meno di non avere una buona ragione. Se usate Windows, disattivate l'opzione che nasconde le estensioni dei tipi di file conosciuti: essa permette a cavalli di Troia di entrare sotto mentite spoglie. Disinstallate lo Scripting Host di Windows

se potete farne a meno. Se non potete, cambiate almeno le associazioni dei vostri file, in modo che i file script non sono automaticamente inviati allo Scripting Host se fate doppio clic su di essi.

Software antivirus e anti-spyware: usateli, che si tratti di un programma combinato o di due applicazioni distinte. Scaricate e installate i vari aggiornamenti, almeno ogni settimana e ogni volta che sentite di un nuovo virus in circolazione. Alcuni prodotti antivirus controllano la presenza di aggiornamenti in modo automatico. Attivate quella funzione e impostatela su "quotidianamente".

Firewall: spendete 50 dollari per un Network Address Translator: dovrebbe andare bene anche in modalità di default. Sul vostro portatile, usate un firewall software. Se potete, nascondete il vostro IP. Non c'è motivo di permettere alcuna connessione in entrata proveniente da chicchessia.

Crittografia: installate un programma per crittografare file e e-mail (come PGP). Crittografare tutte le vostre e-mail o il vostro intero hard disk è poco realistico, ma certa posta è troppo privata per essere inviata in chiaro. Allo stesso modo, certi file sono troppo personali per essere lasciati privi di crittografia.

Nessuna delle contromisure descritte è infallibile. Se la polizia segreta vuole prendere di mira i vostri dati o le vostre comunicazioni, non c'è misura che tenga fra quelle elencate. Ma queste sono buone precauzioni per una certa "igiene di rete", e vi renderanno un bersaglio più difficile del computer del vostro vicino. E anche se seguite solo alcune misure di base, non dovrete avere problemi.

Purtroppo mi tocca usare Microsoft Windows e Office, ma per il web uso Opera, ed Eudora per l'e-mail. Uso Windows Update per ottenere immediatamente le patch e installare altre patch quando ne vengo a conoscenza. Il mio software antivirus si aggiorna regolarmente. Tengo il mio computer abbastanza pulito e cancello i programmi che non mi servono. Effettuo diligentemente il backup dei miei dati e conservo offline quei file che non mi servono più.

Sono sospettoso fino a essere quasi paranoico per quanto riguarda gli allegati nelle e-mail e i siti Web. Canello cookie e spyware. Osservo gli URL per essere sicuro di essere dove sono, e non mi fido della posta indesiderata. Non mi curo molto delle password a bassa sicurezza, ma cerco di avere delle ottime password per account che hanno a che fare con i soldi. Continuo a non fare banking online. Ho il mio firewall impostato per rifiutare qualsiasi connessione in entrata. E spengo il computer quando non lo uso.

Questo è tutto, essenzialmente. Davvero, non è così arduo. La parte più difficile è sviluppare un certo intuito per quando riguarda e-mail e siti Web, ma quello viene con l'esperienza.

Altri hanno contestato questi consigli:
<<http://www.getlucky.net/archives/000145.html>>
<http://www.berylliumsphere.com/security_mentor/2004/12/heres-another-really-good-twelve.html> oppure <<http://makeashorterlink.com/?Z3772560A>>

Il mio articolo originario sul tema in oggetto:
<<http://www.schneier.com/crypto-gram-0105.html#8>>

Questo articolo è originariamente apparso su CNet:
<http://news.com.com/Who+says+safe+computing+must+remain+a+pipe+dream/2010-1071_3-5482340.html> or <<http://makeashorterlink.com/?V6872560A>>

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

Commenti dei lettori

Da: Sitaram Chamarty <sitaram@atc.tcs.co.in>

Oggetto: Le macchine per il Voto Elettronico

Se da un lato mi trova concorde con molto di ciò che lei ha affermato in merito al voto elettronico e aspetti correlati, vi sono però alcune cose, che lei potrebbe già conoscere o meno, che vorrei aggiungere alla discussione.

(1) Malgrado il voto in India non abbia "proposizioni" da votare, capita che alcune volte vengano raggruppate insieme elezioni statali e federali. Infatti è possibile che si indichi un'elezione *prima del dovuto* se il partito in carica perde il controllo prima della fine del suo mandato. Se non fosse per questo, tutte le elezioni sarebbero precise come un orologio (come negli USA) e allora forse tutte le elezioni statali e federali avrebbero luogo nello stesso momento.

(2) Ancora più importante, la tecnologia EVM usata in India è, a mio modesto avviso, di molto superiore a quella utilizzata negli Stati Uniti. Vi è un buon confronto tecnico dei due sistemi all'indirizzo <<http://techaos.blogspot.com/2004/05/indian-evm-compared-with-diebold.html>> (salti pure i primi paragrafi se vuole). Non è un sito ad alto profilo, è solo il blog personale di qualcuno, ma i fatti parlano da soli e possono essere verificati indipendentemente, per cui suppongo sia OK.

(3) Infine, di grande aiuto è il fatto che la nostra commissione elettorale <<http://www.eci.gov.in/>> sia tenacemente indipendente e abbia il mandato costituzionale e il coraggio di scontrarsi spesso con il partito al governo! Un altro contributo viene dal fatto che le macchine sono realizzate da organizzazioni del settore pubblico. CEO di aziende costruttrici delle macchine EVM che promettono di "dare il voto" a un certo partito e cose simili non sembrano esserci qui ;-)

Da: Jeremy Epstein <jeremy.epstein@cox.net>

Oggetto: Le macchine per il voto elettronico

Lei ha scritto: "Nella Contea di Fairfax (Virginia), nel 2003, un errore di programmazione nelle macchine per il voto ha fatto sì che sottraessero misteriosamente 100 voti dai totali di un certo candidato."

In realtà andò peggio di così. Non erano 100 voti, ma uno ogni cento (cioè l'1%) in una corsa elettorale dove il margine era l'1%.

Inoltre, per quanto riguarda il fatto che il codice delle macchine per il voto debba essere pubblico, non sono d'accordo per due ragioni.

Primo, se dobbiamo avere dei tracciati su carta verificabili dall'utente (o qualsiasi sinonimo da lei usato), allora non importa quel che fa il software. Se non funziona a dovere, possiamo individuare l'errore in fase di secondo conteggio.

Secondo, stabilisce un limite nel luogo sbagliato. Se vogliamo il codice open source, esso dà la possibilità a gente come l'ITAA di dire che siamo un manipolo di geek che non credono nei diritti di proprietà. E infatti non c'è ragione del perché le macchine per il voto elettronico *non debbano* competere in fatto di usabilità, affidabilità, ecc.; cosa che può richiedere un codice chiuso. Lasciamo che sia il libero mercato a governare in questo caso! Non sto dicendo che il codice debba essere per forza proprietario per essere sicuro (sono d'accordo con lei su questo). Nei suoi articoli, lei ha persino fatto notare come non vi sia una differenza accuratamente distinguibile nella sicurezza di Windows e Linux, per prendere ad esempio il confronto più diffuso.

In merito all'ottenere ciò che vogliamo, noi nella comunità della sicurezza dovremmo attenerci a quel che importa davvero (tracciati cartacei di verifica), e tenerci alla larga dal campo minato politico inerente all'accesso al codice sorgente.

Da: Thomas Stalzer <electroemporium@yahoo.com>

Oggetto: Le macchine per il Voto Elettronico

Ho notato qui alcune cose relative alle elezioni italiane che, se da un lato possono sembrare un po' "eccessive", funzionano davvero. Il sistema è in uso da anni e anni, e fundamentalmente funziona così:

Le schede per votare sono cartacee, e vengono separate in varie sezioni, ogni scheda è identificata da un colore, e riguarda esclusivamente certe cose, come i rappresentanti, il presidente, i referendum, e via dicendo. Le risposte vengono segnate con una "X" bella grossa, e vi sono degli spazi dove scrivere il nome del candidato quando richiesto. Una volta finito di votare, vi sono delle urne di diversi colori in cui vengono disposte le schede corrispondenti. In questo modo si riduce il rischio e l'impatto di schede adulterate, per come la vedo io.

I vari partiti addirittura inviano per posta delle linee guida su come indicare correttamente la propria preferenza sulla scheda. Osservate la figura, seguite la figura... Persino chi è quasi analfabeta riesce a capire come funziona. E dal momento che il sistema di voto è identico in tutto il paese, le varie stazioni televisive spendono parecchio tempo in "mini-lezioni" che spiegano come tutto questo funzioni. E lo fanno persino in prima serata! E a mano a mano che le elezioni si avvicinano, è impossibile evitare queste trasmissioni.

Ma il vero segreto sta nei conteggi. Mia moglie ha lavorato come presidente di seggio, e questa parte del lavoro mi meraviglia sempre. Le varie schede vengono contate manualmente, con la diretta partecipazione e sotto l'osservazione dei vari partiti politici. Ogni partito deve verificare e concordare sui conteggi.

Ovviamente un tale lavoro è intensissimo, alla faccia della partecipazione dei votanti! E certo, il personale impiegato viene pagato, per cui tutto il processo non è proprio economico. Ma non mi può neanche dire che sia meno efficace di tutte quelle macchine di cui lei e tutti quanti avete parlato a lungo. E siccome a far pratica si migliora, i risultati elettorali arrivano più velocemente di quanto si pensi.

È un sistema perfetto? Certamente no. Sono sicuro che sia possibile trovare delle magagne, ma mi sembra che ciò implicherebbe trascuratezza reciproca o collusione di interessi opposti, in un paese dove la politica è il secondo sport nazionale. Almeno è possibile effettuare ulteriori conteggi finché tutti si trovano concordi.

Certo, l'Italia si è beccata molte critiche per i suoi 50 e più governi esecutivi dalla Seconda Guerra Mondiale in poi, e sicuramente l'Italia non è scevra dalla corruzione; però credo che su questo aspetto abbiano fatto qualcosa di sensato. Almeno di questo gli italiani non si lamentano, e loro non sono certo restii a lamentarsi quando i loro uomini politici fanno qualcosa di poco gradito!

Da: Geoff Kuenning <geoff@cs.hmc.edu>

Oggetto: La sicurezza informatica e la responsabilità

Se non lo ha mai letto, dovrebbe rintracciare l'articolo del CACM sulla storia delle caldaie a vapore che apparvero ad un certo punto negli anni Ottanta. Un breve riassunto è questo: dopo che fu inventata la forza vapore, moltissime caldaie presero ad esplodere e a far danni. Nel Regno Unito il problema fu affrontato con una serie di norme. Negli Stati Uniti, i sostenitori del libero mercato riuscirono a sostenere che la legge sulla responsabilità fosse più che sufficiente: i costruttori di caldaie avrebbero perso alcune cause e avrebbero avuto poi un incentivo a sviluppare caldaie più sicure.

Il risultato fu che le morti connesse alle esplosioni di caldaie scesero quasi a zero nel Regno Unito e continuarono invece a tassi elevati per altri 20 anni negli Stati Uniti, finché alla fine abbiamo ceduto e regolamentato l'industria.

Il problema della responsabilità come meccanismo di feedback è che il feedback negativo è fortemente sconnesso dall'azione originaria. La responsabilità può essere d'aiuto, ma non mi pare del tutto chiaro

come il rendere Microsoft responsabile di tutti i worm nel mondo possa fare in modo che Microsoft inizi a sviluppare software sicuro.

Da: "Joe Patterson" <jpatterson@asgardgroup.com>

Oggetto: I playoff di baseball (World Series) e la sicurezza

Poche centinaia di poliziotti in borghese sembreranno fuori posto, potranno essere nervosi e non guardare la partita; non esulteranno, fischieranno, né gesticoleranno come farebbe un qualsiasi tifoso. Per cui anche in questo caso andiamo incontro a problemi:

1) È difficile riconoscere a vista poche centinaia di persone. Come impedirebbe ai poliziotti in borghese di spendere molto del loro tempo a controllarsi l'un l'altro? Quale sistema di autenticazione ci può essere per far in modo che un poliziotto si fidi dell'altro? Quanto è semplice da falsificare quel sistema di autenticazione? Questo problema può essere risolto assegnando determinate aree ad ogni poliziotto, e accertandosi che ogni poliziotto conosca personalmente e possa riconoscere tutti gli altri poliziotti nella sua area e nelle aree adiacenti (che è come viene fatto nella maggior parte dei casi, ma è una considerazione importante a prescindere).

2) E come la mettiamo con quelle persone fra il pubblico che, consapevoli delle problematiche di sicurezza, possano credere che i poliziotti in borghese si stiano comportando stranamente e possano essere terroristi? Quanti di questi spettatori riporteranno "attività sospetta"? Quanti di questi rapporti ci vorranno prima che *qualsiasi* rapporto di "attività sospetta" venga ignorato perché magari si tratta soltanto di uno dei poliziotti in borghese?

(Si noti come questi due problemi siano sfaccettature della medesima problematica. I terroristi sono rari. Sicuramente ci sono meno terroristi che poliziotti. Almeno lo speriamo tutti! Tuttavia, poliziotti in borghese si comportano in maniera piuttosto simile a terroristi. Aggiungere altri poliziotti in borghese offre più "scarto" ai terroristi, aumentando il numero di falsi positivi. Quando il livello di rumore diventa sufficientemente elevato, i segnali minori sono indistinguibili dall'assenza di segnale).

3) Non che renda le cose ancora peggiori, ma anche i terroristi operano un riconoscimento comportamentale. Un terrorista addestrato *dovrebbe* essere in grado di capire quali, fra gli spettatori, sono poliziotti. Naturalmente, con la "popolarità" dei bombardamenti suicidi come arma terroristica, i "buoni" hanno un vantaggio: una sorta di evoluzione al contrario. I terroristi che fanno male il loro lavoro potranno essere catturati o tenuti alla larga. Quelli bravi si toglieranno dal gruppo dei nemici.

Ho il sospetto che un metodo migliore potrebbe essere quello di avere un numero inferiore di poliziotti *in uniforme*, e molti osservatori addestrati dotati di impianti di sorveglianza (menti preparate e occhi addestrati che usano la tecnologia come moltiplicatore di forza). Questo può dare il beneficio in più di vedere quali persone sembrano *più* nervose in presenza dei poliziotti in uniforme.

Da: Rick Smith <rick@cryptosmith.com>

Oggetto: Fax falsificati

I fax sono semplici da falsificare, specialmente se si sa come dovrebbe apparire il documento originale. La storia della prigione di West Memphis va ben oltre questo -- il documento presentava ovvi elementi che lo classificavano come alterato, secondo le notizie riportate dallo Huntsville Times.

Il problema sottostante è che nessuno nella prigione era responsabile della verifica dei documenti di rilascio. Secondo le notizie, le scarcerazioni prevedevano decisioni prese sia dal personale del front office, sia da quello del back office. Quelli del back office hanno presunto che il front office non avrebbe inoltrato a loro l'ordine di scarcerazione (via fax) a meno che non fosse legittimo. Apparentemente quelli del front office hanno presunto che il back office avrebbe controllato l'ordine.

Non è la prima volta che dei fax fasulli hanno fatto liberare dei detenuti. In questo caso, come in molti altri casi, sarebbe bastata una telefonata per scoprire l'inganno.

Da: John Wilson <tug@wilson.co.uk>
Oggetto: Il Canile: La Contea di Merced

La "wayback machine" conserva la pagina originale:
<<http://web.archive.org/web/20040117090053/http://web.co.merced.ca.us/elections/touchvote.html>> oppure <<http://makeashorterlink.com/?Q6972660A>>

Da: Mel Beckman <mel@becknet.com>
Oggetto: Il commento di Lexar

Ho pensato che le sarebbe interessata la mia esperienza con Lexar per quanto riguarda il loro Secure JumpDrive difettoso. Ho acquistato il Secure JumpDrive versione 1.0 e l'ho consigliato ad uno dei miei clienti, che ne ha comprati a decine. Quando la storia di @stake è saltata fuori, ho contattato Lexar, che stava recentemente vendendo a prezzi stracciati i vecchi drive 1.0 nei negozi CompUSA... con il numero di versione 1.0 rimosso dalla confezione, ma con la pubblicità CompUSA che sosteneva fossero drive 2.0! CompUSA sta ancora vendendo quei drive difettosi e nessuno della direzione di CompUSA mi richiamerà, suppongo.

Ho chiesto a Lexar di sostituire il mio drive con un modello 2.0, dato che il 1.0 ha un difetto hardware grave (altro che "lieve"!) e il software 2.0 non gira sul drive 1.0. Dopo aver negato molte volte che vi fossero problemi, dichiarando anche come "solo un hacker molto bravo può penetrare nel drive, per cui consideriamo il drive 1.0 ancora un prodotto sicuro", Lexar si è finalmente decisa a cambiarmi il drive, chiedendo la restituzione di quello difettoso.

L'ultima volta che ho controllato, CompUSA stava ancora vendendo i drive 1.0 avanzati, sempre definiti "Sicuri", ma senza la dichiarazione che montassero il software 2.0 di Lexar.

Fra l'altro, né io né il mio cliente siamo mai stati contattati da Lexar per quanto concerne il problema di sicurezza, e continuano a menare il can per l'aia con il mio cliente, che vuole farsi sostituire il gran numero di drive acquistati.

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

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

La versione italiana è curata da Communication Valley SpA <http://www.communicationvalley.it/>.
Per iscriversi o cancellarsi andare all'indirizzo <http://www.cryptogram.it/>.
I numeri arretrati sono disponibili all'indirizzo <http://www.cryptogram.it/>.
Per informazioni crypto-gram@communicationvalley.it.

Inoltrate liberamente CRYPTO-GRAM a colleghi ed amici che possano trovare 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 Counterpane Internet Security, Inc., e membro del comitato consultivo dell'Electronic Privacy Information Center (EPIC).

Scrive spesso e tiene conferenze in merito alla sicurezza informatica e alla crittografia. Il suo sito Web è all'indirizzo < <http://www.schneier.com> >.

Counterpane Internet Security, Inc. è leader mondiale nel monitoraggio guidato della sicurezza informatica. Gli analisti esperti in sicurezza di Counterpane proteggono reti per aziende inserite nella Fortune 1000 a livello mondiale.

Copyright (c) 2004 by Bruce Schneier.