

CRYPTO-GRAM
15 dicembre 2007

Scritta da Bruce Schneier
Fondatore e CTO di BT Counterpane

Edizione italiana curata da Communication Valley SpA

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:

Come proteggere il proprio computer, i dischi e le unità portatili

Imbrogliare lo scanner di scarpe all'aeroporto di Heathrow

News

Un manuale del campo di detenzione di Guantanamo (Gitmo) è stato diffuso in Internet

Le news su Schneier/BT Counterpane

La sicurezza fra dieci anni

Commenti dei lettori

** ** ** * * * * *

Come proteggere il proprio computer, i dischi e le unità portatili

La sicurezza informatica è difficile. La sicurezza del software, dei computer e delle reti sono tutte battaglie continue fra aggressore e difensore. E in molti casi l'aggressore parte avvantaggiato: egli deve trovare soltanto una falla nella rete, mentre il difensore deve trovare e tappare tutte le falle.

La crittografia è un'eccezione. A meno che non vi scriviate i vostri algoritmi, la cifratura sicura è un affare semplice. In questo caso è il difensore ad avere un vantaggio (matematico): chiavi più lunghe aumentano in maniera lineare il lavoro che deve svolgere il difensore, ma il lavoro che deve sobbarcarsi l'aggressore aumenta in maniera geometrica.

Purtroppo la crittografia non può risolvere molti problemi di sicurezza informatica. Ma uno di questi problemi può risolverlo eccome: la sicurezza dei dati quando non vengono utilizzati. Criptare file, archivi, addirittura interi dischi, è facile.

Questo rende ancora più incredibile il fatto che l'ufficio delle imposte britannico (Her Majesty's Revenue & Customs) abbia perduto due dischi contenenti le informazioni personali di 25 milioni di cittadini inglesi: date di nascita, indirizzi, dati sui conti correnti bancari e numeri di previdenza sociale. Da un lato non si tratta di un incidente molto più clamoroso delle migliaia di altre esposizioni di informazioni private di cui abbiamo letto in questi ultimi anni; la perdita dei dati personali di 26 milioni di veterani americani da parte della US Veteran's Administration è un evento del tutto simile. Ma questo è diventato la Chernobyl della privacy in Gran Bretagna.

Forse la crittografia non è poi così semplice da applicare come sembra, e ad alcuni può essere utile un po' di ABC. Ecco come proteggero il mio portatile.

Sul mercato esistono svariati prodotti per la criptatura di interi dischi. Io utilizzo lo strumento Whole Disk Encryption di PGP Disk per due ragioni: è semplice, ho fiducia nell'azienda e negli sviluppatori di software sicuro (per la cronaca, sono membro del Technical Advisory Board di PGP Corporation).

Il setup richiede solo pochi minuti, dopodiché il programma si esegue in background. Tutto funziona come prima, e il degrado delle prestazioni del computer è insignificante. Solo assicuratevi di scegliere una password sicura (PGP invita all'uso di passphrase, che facilitano di molto le cose) e sarete protetti in caso lasciate il portatile in aeroporto o che ve lo rubino dalla vostra camera d'albergo.

Perché criptare l'intero disco e non soltanto alcuni file critici? Per non doversi preoccupare di file di swap, di file temporanei, di file d'ibernazione, di file cancellati, dei cookie del browser, eccetera eccetera. Non è necessario instaurare una politica complessa per stabilire quali file siano sufficientemente importanti da dover essere criptati. Inoltre, in caso di furto, avrete una risposta semplice ed efficace per il vostro capo o per la stampa: nessun problema, il portatile è criptato.

PGP Disk può anche criptare dischi esterni, il che significa che potete proteggere quel dispositivo USB che utilizzate di solito per trasferire dati da computer a computer. Quando viaggio mi servo di una chiavetta USB per il backup. Questi dispositivi stanno diventando fisicamente sempre più piccoli, ma internamente più capaci. Criptando la mia chiavetta non ho di che preoccuparmi in caso la smarrisca.

Consiglio un'ulteriore complicazione. Una criptatura dell'intero disco significa che chiunque si trovi di fronte al computer ha accesso a tutte le informazioni (può essere una persona che si mette al vostro computer quando vi assentate un momento, un Trojan che ha infettato il computer, e così via). Per far fronte a queste e a simili

minacce, consiglio caldamente una strategia di criptatura a due livelli. Criptate separatamente, con una password diversa, tutti i dati a cui non accedete con regolarità: documenti archiviati, vecchie email, qualsiasi cosa. A me piace utilizzare i file zip criptati di PGP Disk, perché facilitano anche l'esecuzione di backup sicuri (e consente di proteggere quei file prima di masterizzarli su un DVD e spedirli da un capo all'altro del paese), ma è anche possibile servirsi della funzione di disco virtuale criptato per creare un volume distinto e protetto da crittografia. Entrambe le opzioni sono molto facili da impostare e utilizzare.

Tuttavia esistono ancora due scenari contro i quali non si è protetti. Non siete protetti nel caso qualcuno vi rubi il portatile di mano mentre state scrivendo qualcosa seduti in un caffè e non siete protetti nel caso le autorità vi chiedano di togliere la criptatura dai vostri dati.

Quest'ultima minaccia sta diventando sempre più concreta. È da molto tempo che mi preoccupa il pensiero che un giorno, durante un passaggio alla frontiera, un funzionario apra il mio portatile e mi chieda di inserire la password. Naturalmente potrei rifiutarmi, ma le conseguenze potrebbero essere gravi e permanenti. Alcuni paesi, come il Regno Unito, Singapore, la Malaysia, hanno approvato leggi che conferiscono alla polizia l'autorità necessaria per ordinarvi di fornire le vostre password e le chiavi di cifratura.

Per difendersi da entrambe le minacce, riducete al minimo indispensabile i dati contenuti nel portatile. Avete proprio bisogno dell'archivio con le email degli ultimi dieci anni? È proprio necessario che ogni dipendente d'azienda si porti appresso l'intero database clienti? Una delle cose più incredibili della storia dell'ufficio delle imposte britannico è che un impiegato governativo di basso livello abbia inviato per posta una copia dell'intero database infantile nazionale al National Audit Office a Londra. Doveva proprio farlo? Non credo. La migliore difesa contro la perdita dei dati e quella di non avere dati da perdere, tanto per cominciare.

Se questo non funziona, potete provare a convincere le autorità che non siete in possesso della chiave di cifratura. La storia regge meglio se si tratta di un archivio compresso e non del disco intero. Potete dire che state trasportando i file per conto del vostro capo, o che vi siete dimenticati la chiave tempo fa. Però assicuratevi che la data e ora associate ai file siano coerenti con quanto affermate.

Esistono altri programmi di criptatura. Se utilizzate Windows Vista, potreste considerare BitLocker. Tale programma, incorporato nel sistema operativo, può criptare l'intero disco rigido del computer. Ma funziona solo con l'unità C:, quindi non vi sarà d'aiuto in caso di dischi esterni o chiavette USB. Inoltre non può essere usato per creare file zip criptati. Ma è facile da utilizzare, ed è gratuito. Molte persone sono entusiaste di TrueCrypt, un programma gratuito e open source. Io non lo conosco.

Questo articolo è originariamente apparso su Wired.com.

<http://www.wired.com/politics/security/commentary/securitymatters/2007/11/securitymatters_1129>

Perché ha suscitato tanto clamore quel che è accaduto nel Regno Unito? Senza dubbio per la portata dell'evento, che ha colpito il 40% della popolazione inglese. Poi la natura dei dati: conti bancari, in più le informazioni sui bambini. Questo fatto va a riattizzare il

È un sistema certamente più rapido, ma anche più facile da ingannare. La vulnerabilità risiede nel fatto che nessuno controlla se le scarpe che avevate quando siete passati attraverso il metal detector siano le stesse che inserite dopo nello scanner.

Ecco come funziona l'attacco. Supponiamo di avere due paia di scarpe: un paio "pulito" che passa ogni tipo di controllo, e un paio pericoloso (ignoriamo per un momento la stupidaggine stessa dell'analizzare le scarpe, e ammettiamo che una macchina a raggi X possa rilevare il paio di scarpe pericoloso). Indossiamo le scarpe pericolose e mettiamo quelle normali nel bagaglio a mano. Passiamo attraverso il metal detector. Poi, arrivati alla macchina che controlla le scarpe, ci leviamo il paio pericoloso e lo mettiamo nel bagaglio a mano, prendiamo il paio di scarpe "pulito" e lo infiliamo nella macchina a raggi X. Siamo appena riusciti a passare la sicurezza senza che nessuno ci abbia controllato le scarpe.

Questo trucco funziona perché i due sistemi sono dissociati. Intorno allo scanner di scarpe c'è sempre molta gente e molto caos, alla macchina è presente un numero insufficiente di addetti alla sicurezza: nessuno noterà lo scambio.

Agli aeroporti statunitensi le persone sono obbligate a mettere le scarpe nella macchina a raggi X e a camminare attraverso il metal detector senza scarpe, così da garantire che tutte le scarpe siano controllate. Può essere un sistema più lento, ma funziona.

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

News

Dan Bernstein ha scritto uno studio interessante sulle lezioni di sicurezza che ha appreso da gmail.

<<http://cr.yip.to/gmail/qmailsec-20071101.pdf>>

Possibile "talpa" di Hizbullah all'interno di CIA ed FBI.

<<http://newsweek.com/id/70309>>

In precedenza ho parlato di Dan Egerstad, un ricercatore di sicurezza che gestiva una rete di anonimato Tor e che è stato in grado di intercettare molti nomi utente e password di entità piuttosto importanti. La polizia svedese lo ha arrestato il mese scorso.

<<http://www.smh.com.au/news/security/police-swoop-on-hacker-of-the-year/2007/11/15/1194766821481.html>> oppure <<http://tinyurl.com/2ou5df>>

Il mio precedente articolo:

<http://www.schneier.com/blog/archives/2007/09/anonymity_and_t_1.html>

Ecco un buon articolo su ciò che Egerstad ha commesso; è stato pubblicato appena prima dell'arresto.

<<http://www.smh.com.au/news/security/the-hack-of-the-year/2007/11/12/1194766589522.html>> oppure <<http://tinyurl.com/23u4nr>>

Colossus, la macchina di fattorizzazione della Seconda Guerra Mondiale, è di nuovo online.

<<http://news.bbc.co.uk/1/hi/technology/7094881.stm>>

Foto:

<<http://fungu.notlong.com/>>

<<http://deeke.notlong.com/>>

Naturalmente un moderno PC è più veloce.

<<http://news.bbc.co.uk/1/hi/technology/7098005.stm>>

<<http://www.physorg.com/news114422189.html>>

Hacking ai danni di un distributore di bevande: un video con le istruzioni. L'idea è semplice: evitare che la macchina porti a termine un'azione e indurla in uno stato di errore, quindi sfruttare lo stato di errore. In questo esempio, l'hacker impedisce al distributore di rilasciare la bottiglietta. La macchina restituisce il denaro, ma la bottiglia rimane nella cinghia di distribuzione. Poi l'hacker compra una seconda bottiglia e le riceve entrambe.

<<http://www.5min.com/Video/How-To-Hack-a-Soda-Machine-2497>>

Questa storia parla di dischi rigidi venduti con Trojan preinstallati. Non so se sia vero, ma è certamente possibile:

<<http://www.taipeitimes.com/News/taiwan/archives/2007/11/11/2003387202>>

<<http://forum.rpg.net/showthread.php?t=365473>>

Ancora "guerra all'imprevisto". In Australia un uomo è stato buttato fuori da un pub perché stava leggendo un libro intitolato "L'ignoto terrorista".

<http://www.cairnspost.com.au/article/2007/11/15/4555_news.html>

Alla frontiera USA-Canada, un camion dei vigili del fuoco che stava rispondendo a un'emergenza, con tanto di lampeggianti e sirene spiegate, è stato fermato per circa otto minuti.

<<http://www.cnn.com/2007/US/11/14/border.firetruck/>>

Su un autobus a Leeds, la polizia ha colpito un uomo con i taser quando il tizio era in coma diabetico.

<http://news.bbc.co.uk/1/hi/england/west_yorkshire/7096456.stm>

Una mistura di farina e zucchero ha fatto chiudere un aeroporto nel Maine:

<<http://www.seacoastonline.com/apps/pbcs.dll/article?AID=/20071108/NEWS/71108009>> oppure <<http://tinyurl.com/386hle>>

Un musicista di calypso non vedente e il suo gruppo sono stati fatti scendere da un aereo:

<<http://www.guardian.co.uk/terrorism/story/0,,2218533,00.html>>

Un uomo ebreo fatto scendere da un treno perché stava pregando:

<<http://www.ynetnews.com/articles/0,7340,L-3477136,00.html>>

Una squadra di artificieri a Sarasota, Florida, viene chiamata per far detonare una... macchina da scrivere:

<<http://www.heraldtribune.com/article/20071203/BREAKING01/71203010>>

La paura sta vincendo. Non permettete che vi terrorizzino!

<http://www.schneier.com/blog/archives/2006/08/what_the_terror.html>

All'inizio non ho dato molto credito a questa storia di dinamite fasulla che provoca un'evacuazione, considerandola un ennesimo esempio di reazione istintiva eccessiva di fronte a una minaccia inesistente. Evacuare tutte le persone nel raggio di un miglio sembrava eccessivo, anche in caso di dinamite vera.

<<http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2007/11/21/MN00TGV9P.DTL>>
oppure <<http://tinyurl.com/2dnzlx>>

Ma assumendo che le informazioni in questo articolo siano corrette, può darsi che non sia stata una reazione così eccessiva. Si trattava di un allarme bomba fasullo lanciato intenzionalmente.

<<http://www.ktvu.com/news/14663960/detail.html>>

Nessun controllo affidato a due persone o complicate caratteristiche di sicurezza: nel Regno Unito fino al 1998 era possibile armare reattori nucleari con la chiave di una bicicletta. Sicuramente molta della sicurezza era procedurale. Però...

<<http://news.bbc.co.uk/1/hi/programmes/newsnight/7097101.stm>>

"I passeggeri alla stazione di Lime Street a Liverpool vengono sottoposti a perquisizioni e controlli del bagaglio simili a quanto già avviene negli aeroporti; questo a seguito di nuove e drastiche misure antiterrorismo introdotte ieri. Verranno realizzate barriere di sicurezza, aree a traffico limitato e strutture resistenti alle esplosioni che saranno introdotte negli aeroporti, nei porti e in 250 fra le stazioni ferroviarie più affollate, ha annunciato Gordon Brown". Il titolo della notizia avrebbe dovuto essere: "Il Regno Unito spende miliardi per costringere i terroristi delle linee ferroviarie a guidare un poco più oltre". Stazioni ferroviarie meno affollate, infatti, sono a pochi minuti di auto.

<http://icliverpool.icnetwork.co.uk/0100news/0100regionalnews/tm_headline=lime-street-station-to-face-airport-style-security%26method=full%26objectid=20110268%26siteid=50061-name_page.html>

oppure <<http://tinyurl.com/2zjrxn>>

Un modo brillante di utilizzare Google per craccare password:

<<http://www.lightbluetouchpaper.org/2007/11/16/google-as-a-password-cracker/>>

oppure <<http://tinyurl.com/3b5ftq>>

Un articolo eccellente di John Tehranian sul problema posto dalla legge sul copyright: "Infringement Nation: Copyright Reform and the Law/Norm Gap" [Il Paese dell'Infrazione: la riforma del copyright e il divario fra legge e norma]. L'articolo dimostra come, agendo in maniera assolutamente normale, ogni giorno e molte volte al giorno tutti noi siamo tecnicamente dei trasgressori della legge. Quando le leggi sono così al di fuori delle norme sociali, è tempo di modificarle.

<http://www.turnergreen.com/publications/Tehranian_Infringement_Nation.pdf>

oppure <<http://tinyurl.com/2rgn9c>>

In un altro dei tanti fronti di questa guerra all'imprevisto, ora viene chiesto ai vigili del fuoco di controllare eventuali attività terroristiche mentre svolgono il proprio lavoro. "A differenza della polizia, i vigili del fuoco e il personale medico di emergenza non hanno bisogno di un mandato per avere accesso ogni anno a centinaia di migliaia di abitazioni ed edifici e a ritrovarsi quindi in una posizione che permetta loro di individuare certi comportamenti che potrebbero indicare attività o complotti terroristici". Sicuro, proprio una buona idea mettere la gente in condizione di dover temere i vigili del fuoco...

<http://ap.google.com/article/ALeqM5gek2oSZ_67sh2ukVvXaCGCXzypwD8T3IFL81>

oppure <<http://tinyurl.com/2co9qs>>

Un buon articolo sul crimine cibernetico di contro al terrorismo cibernetico; è ormai parecchio che vado sostenendo le stesse cose.

<http://www.siliconvalley.com/ci_7442979>

Gli attivisti per i diritti degli animali sono costretti a fornire le loro chiavi di cifratura, secondo una nuova legge inglese.

<<http://news.bbc.co.uk/2/hi/technology/7102180.stm>>

Qui vi è qualche notizia in più sulla nuova legge. Se ricordate, fu propinata al pubblico come essenziale per la lotta al terrorismo. È già stata abusata.

<http://www.schneier.com/blog/archives/2007/10/uk_police_can_n.html>

Come raccogliere password: basta implementare un misuratore di forza delle password e invitare le persone a immettere le proprie password per verificarle. Si possono anche raccogliere nomi e indirizzi email.

<<http://www.codeassembly.com/How-to-make-a-password-strength-meter-for-your-register-form/>> oppure <<http://tinyurl.com/2jfu7s>>

Si noti che non sto accusando Codeassembly di rubare password; sto semplicemente dicendo che è possibile raccogliere password in questo modo. Per la cronaca, ecco come scegliere una password sicura:

<http://www.schneier.com/blog/archives/2007/01/choosing_secure.html>

Minaccia da trama cinematografica descritta dalla stampa come minaccia da trama cinematografica.

<<http://www.azstarnet.com/sn/relatedstories/213503.php>>

Alla fine non era altro che finzione (ovviamente).

Un camionista entra nella fabbrica di birra Guinness a Dublino passando dal cancello principale e ruba 450 barili di birra. Morale: cercate di apparire del giro, agendo con naturalezza.

<<http://www.rte.ie/news/2007/1129/guinness.html>>

<<http://www.ireland.com/newspaper/breaking/2007/1129/breaking41.htm>>

Pare che siano stati catturati prima di potersela bere tutta.

<<http://www.ireland.com/newspaper/breaking/2007/1205/breaking85.htm>>

Ogni anno il SANS pubblica un elenco delle 20 vulnerabilità più importanti. È sempre un ottimo elenco, è quest'anno non fa eccezione.

<<http://www.sans.org/top20/>>

L'MI5 dà l'allarme: la Cina sta spiando via Internet. Sono anni che va avanti questa storia, quindi perché l'MI5 lo ha detto pubblicamente (o meglio, ha inviato un documento privato con la certezza che sarebbe stato divulgato)? Al principio ho pensato che qualcuno all'MI5 avesse il dente avvelenato con la Cina. Ora penso che qualcuno all'MI5 fosse frustrato dall'assenza di budget.

<http://business.timesonline.co.uk/tol/business/industry_sectors/technology/article2980250.ece> oppure <<http://tinyurl.com/yptg68>>

La crittografia di Microsoft per le tastiere wireless è stata craccata:

<<http://www.heise-security.co.uk/news/99873>>

<<http://www.dreamlab.net/download/articles/Press%20Release%20Dreamlab%20Technologies%20Wireless%20Keyboard.pdf>>

oppure <<http://tinyurl.com/2qmf8c>>

<http://www.dreamlab.net/download/articles/27_Mhz_keyboard_insecurities.pdf>
oppure <<http://tinyurl.com/3yqdrf>>

Il segretario di stato della California dubita che le macchine per il voto elettronico saranno mai abbastanza valide da poter essere utilizzate per le elezioni nel proprio stato:

<<http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2007/12/02/BASRTMOPE.DTL>>
oppure <<http://tinyurl.com/3dsafg>>

I commenti di Ed Felten:

<<http://www.freedom-to-tinker.com/?p=1232>>

Ho scritto molto sulla questione:

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

<http://www.schneier.com/blog/archives/2006/11/voting_technolo.html>

<http://www.schneier.com/blog/archives/2006/11/more_on_electro.html>

Un attacco man-in-the-middle in un nodo di uscita della rete Tor. Spesso attacchi di questo genere sono puramente teorici; è affascinante vederne uno "in the wild".

<<http://www.teamfurry.com/wordpress/2007/11/20/tor-exit-node-doing-mitm-attacks>> oppure <<http://tinyurl.com/2h8xrv>>

Il tizio afferma di aver semplicemente configurato male il suo nodo Tor. Non conosco abbastanza Tor per commentare questa affermazione.

<<http://forum.fachinformatiker.de/security/110838-ssl-man-middle-ueber-tor-schnueffelei.html#post1013213>> oppure <<http://tinyurl.com/2g6ko9>>

Ho già trattato dell'anonimato e della rete Tor.

<http://www.schneier.com/blog/archives/2007/09/anonymity_and_t_1.html>

Un articolo affascinante su come l'eccessiva dipendenza dalla tecnologia stia danneggiando le truppe americane in Iraq.

<http://www.wired.com/politics/security/magazine/15-12/ff_futurewar>

<http://www.schneier.com/blog/archives/2007/12/an_overdependen.html#c222154>

oppure <<http://tinyurl.com/2bpob4>>

Un nuovo, bizzarro rischio di sicurezza: le coperte.

<<http://www.news.com.au/perthnow/story/0,21598,22860627-2761,00.html>>

Scatole del Monopoli "speciali" per i prigionieri di guerra durante la Seconda Guerra Mondiale contenenti, fra l'altro, denaro vero:

<<http://www.boingboing.net/2007/11/20/pow-editions-of-mono.html>>

Un interessante post su come aggirare i CAPTCHA:

<<http://www.codinghorror.com/blog/archives/001001.html>>

Questo gruppo è il migliore per sconfiggere i CAPTCHA:

<<http://www.ocr-research.org.ua/index.html>>

Lo "Handbook of Applied Cryptography" [Manuale di Crittografia Applicata] è disponibile online... legalmente. È un buon libro, che val la pena scaricare.

<<http://www.cacr.math.uwaterloo.ca/hac/index.html>>

Un adolescente registra segretamente l'interrogatorio a cui viene sottoposto in una stazione di polizia; come conseguenza un investigatore è stato riconosciuto colpevole di

spergiuro. A mio avviso questo genere di falsa testimonianza capita molto più spesso di quanto immaginiamo. Se esiste un luogo in cui vorrei che le telecamere filmassero in continuazione sono proprio le stanze degli interrogatori delle centrali di polizia.
<<http://abcnews.go.com/TheLaw/wireStory?id=3968795>>

La polizia locale sta mettendo degli adesivi gialli sulle auto che contengono pacchi voluminosi e visibili, facilitando il lavoro dei ladri, che possono meglio individuare le auto che val la pena attaccare.
<<http://www.rockdalecitizen.com/print.asp?SectionID=2&SubSectionID=2&ArticleID=453>> oppure <<http://tinyurl.com/2cwxx7>>

Un interessante studio sugli effetti delle leggi statunitensi che obbligano a divulgare falle di sicurezza.
<http://www.law.berkeley.edu/clinics/samuels/cso_study.pdf>

In Germania i progetti per il caveau segreto di una banca sono stati trovati nella spazzatura.
<http://today.reuters.com/news/articlenews.aspx?type=oddlyEnoughNews&storyid=2007-12-07T051401Z_01_L06102154_RTRUKOC_0_US-BUNDESBANK-SAFE.xml> oppure <<http://tinyurl.com/2a2say>>

Un articolo del "Time Magazine" sugli hacker cinesi:
<<http://www.time.com/time/magazine/article/0,9171,1692063,00.html>>

"Security Question", un racconto breve di Ramon Rozas III.
<<http://www.everydayfiction.com/security-question-by-ramon-rozas-iii/>>

** *** *****

Un manuale del campo di detenzione di Guantanamo (Gitmo) è stato diffuso in Internet

Un manuale del 2003 dal titolo "Camp Delta Standard Operating Procedures" [Procedure operative standard di Camp Delta] è stato diffuso in Internet. Si tratta dello stesso manuale che l'ACLU ha cercato di ottenere intentando causa contro il governo. Lascio ad altri discutere sulla legalità di alcune delle procedure; sul mio blog ero interessato più ai commenti in materia di sicurezza.

Si veda, per esempio, questo passaggio a pagina 27.3:

"(b) All'arrivo si passerà dal cancello inserendo il numero (1998) nel lucchetto a combinazione.

"(c) Procedere alla scatola di giunzione con il numero (7012-83) e aprire la scatola. Il numero per lo sblocco della scatola dell'interruttore è (224)".

Moltissimi altri commenti online da parte dei lettori.

Il manuale:

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

Altri articoli:

<<http://www.nytimes.com/2007/11/16/washington/16gitmo.html?ex=1352869200&en=76e443e8322c06f9&ei=5090&partner=rssuserland&emc=rss>>

oppure <<http://tinyurl.com/28zyqm>>

<<http://www.wired.com/politics/onlinerights/news/2007/11/gitmo>>

Il post nel mio blog:

<http://www.schneier.com/blog/archives/2007/11/gitmo_manual_le_1.html>

** *** *****

Le news su Schneier/BT Counterpane

Ho partecipato a uno scambio domanda-risposta sul blog Freakonomics. Niente che i lettori abituali di questo blog non abbiano già sentito prima, ma è stata comunque un'esperienza divertente.

<<http://freakonomics.blogs.nytimes.com/2007/12/04/bruce-schneier-blazes-through-your-questions/>> oppure <<http://tinyurl.com/2zan6q>>

C'è anche un thread su Slashdot a riguardo:

<<http://it.slashdot.org/it/07/12/04/2128256.shtml>>

** *** *****

La sicurezza fra dieci anni

Questa è una conversazione fra il sottoscritto e Marcus Ranum. Solitamente pubblico solo la mia metà di questi scambi di vedute. Ma dato che questo scambio in particolare presenta molti punti interconnessi fra loro, ha molto più senso includere l'intero articolo.

Bruce Schneier: Le previsioni sull'argomento sono al tempo stesso semplici e ardue. Roy Amara dell'Institute for the Future una volta disse: "tendiamo a sopravvalutare l'effetto di una tecnologia nel breve termine e a sottovalutarlo nel lungo periodo".

La Legge di Moore è semplice: nel giro di 10 anni, i computer saranno 100 volte più potenti. Il mio computer da scrivania starà in un cellulare, avremo dovunque una connessione wireless gigabit, e reti personali collegheranno i nostri sistemi informatici e i servizi remoti a cui ci iscriveremo. Altri aspetti del futuro sono molto più difficili da prevedere. Non credo che esista qualcuno in grado di prevedere che cosa porteranno le proprietà emergenti di una capacità di calcolo cento volte maggiore: nuovi utilizzi per i computer, nuovi paradigmi di comunicazione. Un mondo cento volte più potente sarà diverso, in modi che si riveleranno sorprendenti.

Ma attraverso la storia e guardando al futuro, l'unica costante è la natura umana. Sono passati millenni e non è stato ancora inventato un nuovo reato. Frode, furto, scambio di persona e falsificazione sono problemi perenni che esistono sin dagli albori della società. In questi ultimi dieci anni, tali reati si sono trasferiti nel cyberspazio, e nei prossimi dieci migreranno verso qualsiasi piattaforma di calcolo, di comunicazione e di commercio che staremo utilizzando.

La natura degli attacchi sarà diversa, così come i bersagli, le tattiche e i risultati. La sicurezza è al tempo stesso un compromesso e un braccio di ferro, un equilibrio fra chi attacca e chi si difende, e i cambiamenti tecnologici sconvolgono tale equilibrio. La tecnologia potrebbe rendere una certa tattica molto più efficace, o una particolare tecnologia di sicurezza più a buon mercato e quindi più diffusa. Oppure una nuova applicazione emergente potrebbe diventare un bersaglio preferito.

Non vedo nulla, da qui al 2017, che cambierà tutto questo in maniera fondamentale. Tu che ne dici?

Marcus Ranum: penso che tu abbia ragione; a un meta-livello, i problemi sono destinati a rimanere gli stessi. Quel che per me è sconvolgente e scoraggiante è che anche le nostre risposte a tali problemi rimangono le stesse, malgrado la loro inefficacia sia più che evidente. Siamo nel 2007 e ancora pare non abbiamo accettato il fatto che:

- * Non è possibile che del software pessimo diventi affidabile continuando ad applicarvi delle patch.
- * Non si dovrebbero mescolare sistemi di produzione con sistemi non di produzione.
- * È davvero necessario sapere quel che sta succedendo nei propri network.
- * Se si fanno girare i propri computer con un runtime model basato sull'esecuzione aperta, si finirà sempre col ricevere virus, spyware e cavalli di Troia.
- * Si possono approvare leggi sulla chiusura delle porte della stalla dopo che sono scappati i cavalli, ma questo non servirà a far tornare i cavalli nella stalla.
- * La sicurezza deve essere intrinseca al progetto, come parte di un piano sistematico volto all'affidabilità; non dev'essere aggiunta e adattata alla meno peggio in un secondo momento.

L'elenco potrebbe continuare per parecchie pagine, ma sarebbe troppo deprimente. Sarebbe "la lista di Marcus delle cose ovvie che tutti conoscono ma nessuno accetta".

Hai dimenticato un aspetto importante del problema: nel 2017 i computer saranno ancora più essenziali per le nostre vite, per l'economia e le infrastrutture.

Se tu hai ragione sul fatto che il crimine rimane una costante, e io ho ragione sul fatto che le nostre risposte in merito alla sicurezza informatica continuano a essere inefficaci, allora il 2017 sarà molto meno "divertente" di quanto lo sia stato il 2007.

Non ho dato molto credito ai concetti di guerra cibernetica e di terrore cibernetico. Quella scarsa considerazione veniva motivata dalla mia osservazione secondo cui la natura improvvisata e "a patchwork" di moltissimi sistemi informatici funzioni essa stessa da misura difensiva, e che gli attacchi nel mondo reale continuano a essere più efficaci economicamente e più pratici da realizzare per scopi terroristici.

Vorrei ufficialmente modificare un poco la mia posizione: ritengo che entro il 2017 sarà molto più probabile che avvengano guasti catastrofici all'interno di infrastrutture critiche. Probabilmente però non per mano di terroristi; è assai più probabile che vi sarà un pauroso black-out perché un sistema critico era collegato a un sistema non critico che a sua volta era collegato a Internet così che qualcuno potesse accedere a MySpace, e che quel sistema secondario si sia beccato un malware. Oppure sarà un software incomprensibilmente complesso, pieno di cerotti e patch, che crollerà quando un hacker "semplicemente curioso" spingerà il pulsante virtuale sbagliato. Vi sono delle tendenze che non promettono nulla di buono; tutti gli indicatori puntano verso un sistema più complesso, meno padroneggiato e più interdipendente. Con un'infrastruttura simile, chi ha bisogno di nemici?

A te preoccupa il fatto che i criminali continueranno a penetrare nel cyberspazio, e a me preoccupa che complessità, cattivo design e pessima gestione saranno lì ad attenderli.

Bruce Schneier: mi pare che abbiamo già visto quel genere di guasto critico di cui parlavi. Il black-out dell'agosto 2003 che ha colpito buona parte del nordest degli Stati Uniti e del Canada (50 milioni di persone) fu provocato da un bug software.

Le cose continueranno a peggiorare, sono d'accordo. La complessità è il peggior nemico della sicurezza, e Internet (e i computer e i processi a essa collegati) sta diventando sempre più complessa. Per cui le cose stanno peggiorando anche se la tecnologia della sicurezza sta migliorando. Si potrebbe dire che quelle insicurezze critiche sono un'altra proprietà emergente del mondo cento volte potenziato del 2017.

Sì, i sistemi IT saranno sempre più essenziali per la nostra infrastruttura: l'home banking, le comunicazioni, i servizi di base, la difesa, tutto quanto.

Nel 2017 le interconnessioni saranno talmente critiche che probabilmente per una organizzazione terroristica sarà conveniente e a basso rischio sferrare attacchi attraverso Internet. Oggi derido le chiacchiere sul terrorismo cibernetico, ma non credo che lo farò da qui a dieci anni.

Se da una parte le tendenze di maggiore complessità e di pessima gestione non sono affatto buone, esiste un altro trend che punta a una maggiore sicurezza, ma non piacerà né a te né a me. È il trend dell'Information Technology come servizio.

Nel 2017 le persone e le aziende non acquisteranno computer e connessione come lo stanno facendo oggi. Il mondo sarà dominato dalle grandi imprese di telecomunicazioni, dagli Internet Provider e da compagnie di integrazione dei sistemi, e l'informatica sarà sempre più considerata come un servizio pubblico. Le aziende venderanno servizi, non prodotti: servizi email, servizi di applicazioni, servizi di intrattenimento. Stiamo iniziando a vedere oggi questa tendenza e prenderà sempre più piede nei prossimi dieci

anni. Tutto ciò influisce sulla sicurezza per il fatto che nel 2017 le persone e le aziende non avranno molto controllo sulla propria sicurezza. Ogni cosa verrà gestita a livello di Internet Provider e di backbone. I giorni spensierati dei PC di uso generale saranno in gran parte un ricordo. Pensiamo al modello dell'iPhone: si riceve quel che Apple decide di fornire, e se si cerca di modificare il telefono, Apple può vanificare lo sforzo con un semplice aggiornamento software. A noi "geek" non piacerà, ma è il futuro. Internet è sostanzialmente commercio, e il commercio non potrà sopravvivere in altro modo.

Marcus Ranum: Hai ragione per quanto riguarda lo spostamento verso i servizi: è il sistema definitivo per fidelizzare i clienti.

Se si è capaci di fare in modo che sia difficile per il cliente riottenere i propri dati dopo che li si è tenuti per un po' di tempo, si riuscirà efficacemente a impedire che il cliente se ne vada. Naturalmente ai clienti si dirà "fidatevi di noi, le vostre informazioni sono al sicuro", e per loro questa sarà una risposta. I sistemi back-end che alimenteranno il futuro dell'informatica dei servizi saranno pieni di vulnerabilità come quelli attuali. L'informatica dei servizi, inoltre, non sarà affatto in grado di affrontare il problema della fiducia transitiva a meno che le persone non comincino a passare a un endpoint rappresentato da una piattaforma informatica più affidabile.

È questo il problema della direzione che stiamo prendendo: gli endpoint non sono destinati a migliorare. La gente è attratta dalle appliance perché aggirano l'onere dell'amministrazione di sistema (che, nell'ambiente della sicurezza di oggi, equivale a "un inferno di patch infinite"), ma sotto la superficie attraente delle appliance troveremo la medesima accozzaglia di insicurezze che abbiamo avuto con le macchine desktop di uso generale. Infatti, lo sviluppo di appliance azionate da sistemi operativi di uso generale rende davvero concreta la possibilità di una monocultura software. Da qui al 2017, pensi che l'ingegnerizzazione dei sistemi progredirà al punto in cui non vedremo un'azienda lanciare un nuovo prodotto e creare istantaneamente una base di installato di un milione e passa utenti con privilegi di root? Io non credo, e questo mi spaventa.

Pertanto, se stai dicendo che la tendenza è quella di continuare a mettere tutte le uova in un solo paniere e di fidarsi sconsideratamente di quel paniere, mi trovi in totale accordo.

Un'altra tendenza che vedo peggiorare è il know-how del governo in ambito IT. Al ritmo con cui l'outsourcing ha istupidito la forza lavoro federale, entro il 2017 non sarà rimasto un solo dipendente del governo che saprà far qualcosa con un computer se non navigare in Internet e far girare PowerPoint. Scherzi a parte, il risultato è che l'infrastruttura governativa critica sarà quasi interamente gestita dall'esterno. Le implicazioni strategiche di un cambiamento del genere mi hanno da sempre turbato; significa una perdita di controllo sulle informazioni, sulle risorse e sulle comunicazioni.

Bruce Schneier: sugli endpoint che non miglioreranno hai assolutamente ragione. Ho scritto più e più volte che misure come l'autenticazione a due fattori non renderanno l'Internet banking più sicuro. Il problema è che se qualcuno ha inserito un Trojan nel tuo computer, non importa in quanti modi ti autentichi presso il server di banking; il Trojan inizierà a effettuare transazioni illecite subito dopo l'autenticazione.

Accade la stessa cosa con molti dei nostri protocolli sicuri. SSL, SSH, PGP, ecc., tutti presumono che gli endpoint (cioè i due estremi della comunicazione) siano sicuri, e che la minaccia si trovi nel sistema di comunicazione. Ma sappiamo che i veri rischi sono gli endpoint.

A dominare l'informatica del 2017 sarà un tentativo incauto di risolvere questo problema. Ho parlato di software-come-servizio che, come tu hai sottolineato, è in realtà un trucco che permette alle aziende di trattenerne i propri clienti nel lungo periodo. Io ho fatto l'esempio di iPhone, che raggiunge il medesimo obiettivo grazie alle rigide regole che stabiliscono chi può scrivere software per tale piattaforma e chi no. Potremmo anche portare l'esempio del Trusted Computing di Microsoft, che viene venduto come misura di sicurezza quando in realtà è un altro meccanismo per impedire che gli utenti passino a software "non autorizzato" o ad altri sistemi operativi.

Mi viene in mente l'isteria antiterroristica immediatamente successiva all'11 settembre: abbiamo confuso la sicurezza con il controllo, e invece di costruire sistemi che garantiscano sicurezza vera, abbiamo costruito sistemi di controllo. Si pensi ai continui controlli dei documenti d'identità in ogni luogo, alla no-fly list, alle intercettazioni senza mandato, alla sorveglianza all'ingrosso, al data mining e a tutti i sistemi per controllare sommozzatori, piloti di aerei privati, attivisti per la pace e altri gruppi di persone. Tutti questi sistemi offrono una sicurezza insignificante, ma mettono nelle mani del governo un livello di controllo incredibile.

L'informatica sta andando nella stessa direzione, solo che questa volta è l'industria a volere il controllo sui suoi utenti. Ce lo venderanno come sistema di sicurezza (potrebbero addirittura essersi autoconvinti che migliorerà davvero la sicurezza), ma è fondamentalmente un sistema di controllo. Alla lunga finirà col nuocere alla sicurezza.

Immaginiamo di vivere in un mondo di Trustworthy Computing, in cui nessun software può girare sulla vostra macchina Windows a meno che Microsoft non lo approvi. Quell'istupidimento di cui parli non sarà un problema, perché la sicurezza non sarà nelle mani dell'utente. Microsoft reclamizzerà questo come la fine del malware, finché un hacker non scoprirà come far approvare il proprio software. Ecco il problema di ogni sistema che si appoggia sul controllo: una volta trovato il modo di compromettere il sistema di controllo, si è a posto. Per cui, invece di un triliardo di noiosi worm, nel 2017 ne vedremo comparire meno, ma saranno dei super-worm ancora peggiori che aggireranno le nostre difese.

Entro quella data, tuttavia, saremo pronti a iniziare a costruire della vera sicurezza. Come hai fatto notare, le reti saranno talmente incorporate nella nostra infrastruttura critica (e probabilmente sarà già accaduto qualche vero disastro entro il 2017), che non avremo altra scelta. La questione è: quanto dovremo smantellare e ricostruire daccapo per farlo nella maniera giusta?

Marcus Ranum: Concordo con la tua visione negativa del futuro. È ironico che gli "hacker" della controcultura abbiano permesso (offrendo una scusa) l'esistenza dell'ambiente software di oggi basato sulla dinamica esecuzione-patch-esecuzione-patch-riavvio e lo stalinismo del software di domani.

Non credo che inizieremo a costruire della vera sicurezza. Perché la sicurezza vera e propria non è una cosa che si costruisce, ma che si ottiene quando si getta via tutto il resto dell'immondizia come parte del procedimento di design. Il software progettato e costruito per un certo scopo è più costoso da realizzare, ma più economico da mantenere. Il giudizio prevalente sul tasso di redditività del capitale investito in un software non tiene conto del processo di patching e del downtime dovuto al patching; perché se lo facesse, i conti non tornerebbero. Nel frattempo ho visto sistemi Internet costruiti all'uopo funzionare per anni senza bisogno di patch perché non si appoggiavano a componenti sovrabbondanti. Dubito che l'industria lo comprenderà.

Il futuro sarà fatto di informazioni prigioniere che gireranno su sistemi back-end costruiti allo scopo. Non sarà un futuro sicuro, perché fornire i propri dati personali è sempre un indebolimento della propria sicurezza. Pochi possiedono la capacità di comprendere la complessità e i principi di buon design necessari a realizzare sistemi affidabili o sicuri. Pertanto, in effetti, l'outsourcing (o altre forme per far diventare la sicurezza il problema di qualcun altro) continuerà a sembrare un'opzione attraente. Non mi sembra un futuro molto roseo. Ed è un peccato, perché è importante fare bene queste cose. Hai ragione quando dici che vi saranno dei disastri nel nostro futuro.

Penso che si tratterà più che altro di incidenti in cui il sistema crolla sotto il peso della sua stessa complessità, e non a causa di aggressioni. Saremo in grado di capire che cosa sarà successo, quando accadranno tali incidenti?

Gente, i comandanti hanno attivato il segnale "allacciarsi le cinture di sicurezza". Si prevedono turbolenze sul nostro cammino.

Questo articolo è originariamente apparso in "Information Security Magazine".

Commenti allo scambio di vedute:

<http://www.channelregister.co.uk/2007/12/04/security_in_2017/>

Il thread su Slashdot:

<<http://it.slashdot.org/article.pl?sid=07/12/03/1840243>>

** ** ** * * * * *

Commenti dei lettori

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

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

** ** ** * * * * *

CRYPTO-GRAM è una newsletter mensile gratuita che offre riassunti, analisi, approfondimenti, e commenti sulla sicurezza (informatica e in generale) e sulla crittografia. I numeri arretrati sono disponibili all'indirizzo <<http://www.schneier.com/crypto-gram.html>>. Per iscriversi, cancellare l'iscrizione o cambiare il proprio indirizzo a cui recapitare la newsletter, visitate sempre <<http://www.schneier.com/crypto-gram.html>>

La versione italiana è curata da Communication Valley SpA

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

Per iscriversi o cancellarsi andare all'indirizzo <<http://www.cryptogram.it/>>

I numeri arretrati sono disponibili all'indirizzo <<http://www.cryptogram.it/>>

Per informazioni <crypto-gram@communicationvalley.it>

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 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>>.

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) 2007 - Bruce Schneier.