

CRYPTO-GRAM
15 gennaio 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-0612.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:

Il sistema automatico di controllo ATS
Telecamere di sorveglianza filmano un assassino a sangue freddo
Le ristampe di Crypto-Gram
Intercettazioni uditive
Tener traccia delle automobili tramite i loro pneumatici
Accordare una licenza ai barcaioli
Un centro commerciale Wal-Mart rimane aperto durante un allarme bomba
News
La NSA aiuta Microsoft con Windows Vista
Il sistema anti-phishing di Microsoft e le piccole imprese
Le sviste del Dipartimento della Motorizzazione della Virginia
Ancora sul codice di Unabomber
Le news di BT Counterpane
Radiotrasmittitori nascosti nelle monete canadesi
Scegliere password sicure
Commenti dei lettori

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

Il sistema automatico di controllo ATS

Se avete fatto viaggi all'estero di recente, siete stati oggetto d'indagini. Vi è stato infatti assegnato un punteggio che indica il tipo di minaccia terroristica che rappresentate. Tale punteggio viene utilizzato dal governo per determinare il trattamento che riceverete al vostro ritorno negli Stati Uniti e anche per altri scopi.

Volete conoscere il vostro punteggio? Non potete. Siete interessati a sapere quali informazioni sono state usate? Non potete saperlo. Volete togliere il vostro nome o chiarire equivoci nel caso siate stati inseriti erroneamente in un'altra categoria? Non è possibile. Volete sapere quali tipi di regole vengono impiegati dal computer per giudicarvi? Anche questa informazione è segreta. Stesso dicasi per il quando e il come verrà utilizzato tale punteggio.

Le agenzie di frontiera statunitensi hanno tacitamente impiegato questo sistema per parecchi anni ormai. Denominato Automated Targeting System, ossia sistema automatico di controllo, esso assegna un "profilo di rischio" alle persone che entrano o lasciano il paese, o che praticano attività di importazione/esportazione. Questo punteggio, e le informazioni utilizzate per stabilirlo, possono essere condivisi con le autorità federali, statali, locali e persino con governi stranieri. Possono venire usati se state cercando un impiego governativo, o se fate richiesta di sovvenzioni, autorizzazioni, contratti o altri benefici. Possono essere passati a organizzazioni non-governative e/o a privati durante un'indagine. In alcuni casi sono ottenibili da fornitori privati, anche quelli che non si trovano negli Stati Uniti. E verranno registrati per quarant'anni.

Di questo programma si conosce ben poco. Le sue linee basilari sono state divulgate dal Federal Register in ottobre. Sappiamo che il punteggio si basa in parte sui dettagli del vostro registro di volo (di dove siete, come avete comprato il biglietto, dove siete seduti, se avete fatto richieste particolari per il pasto) o sui registri della motorizzazione, insieme a informazioni ricavate dalla fedina penale, da watch list e da altri database.

Molti gruppi sostenitori delle libertà civili hanno definito questo programma "kafkiano". Personalmente, la cosa che più mi infastidisce di esso è che sia un totale spreco di denaro.

L'idea di dare in pasto a un computer un ristretto insieme di caratteristiche, per ottenere una sorta di divinazione sulle eventuali inclinazioni terroristiche di un individuo, è a dir poco farsesco. La scoperta di una trama terroristica è frutto di intelligence e investigazioni, non dell'elaborazione dei dati di ognuno su larga scala.

Inoltre, qualsiasi sistema di questo tipo produrrà una tale quantità di falsi allarmi da risultare assolutamente inutilizzabile. Nel 2005 Customs & Border Protection ha esaminato 431 milioni di persone. Presupponendo un modello non realistico in grado di identificare terroristi (e innocenti) con una precisione del 99,9%, rimarrebbero 431.000 falsi allarmi ogni anno.

In realtà il numero di falsi allarmi sarà ben maggiore. La no-fly list è piena di imprecisioni: tutti abbiamo letto di individui innocenti chiamati David Nelson che non possono volare senza prima venire sottoposti a vessazioni per ore e ore. Anche le informazioni delle linee aeree abbondano di errori.

Le probabilità che questo programma venga implementato in sicurezza e con un'adeguata protezione della privacy sono scarse. Lo scorso anno ho partecipato a un gruppo di lavoro governativo per valutare la sicurezza e il livello di privacy di un programma simile sviluppato dalla

Transportation Security Administration, chiamato Secure Flight. Dopo cinque anni e un investimento di 100 milioni di dollari, tale programma non è tuttora in grado di eseguire il semplice compito di confrontare una lista di passeggeri con le informazioni delle watch list antiterrorismo.

Nel 2002 è venuto alla luce un ennesimo programma, chiamato Total Information Awareness, mediante il quale il governo avrebbe raccolto informazioni su ogni cittadino americano e gli avrebbe assegnato un profilo di rischio terroristico. Il Congresso trovò l'idea talmente aberrante che congelò i finanziamenti al progetto. Due anni dopo, e ancora una volta lo scorso anno, il Congresso ha bandito anche Secure Flight, a meno che non sia in grado di superare alcune prove di accuratezza e protezione della privacy.

Infatti si può dire che l'Automated Targeting System è altrettanto illegale (cosa che è stata fatta notare di recente da alcuni membri del congresso); tutti i progetti legge di stanziamento del Dipartimento per la Sicurezza Nazionale proibiscono specificamente al dipartimento l'utilizzo di sistemi di profiling su persone non appartenenti a watch list.

Vi è qualcosa di anti-Americano in un programma governativo che sfrutta criteri segreti per raccogliere dossier su persone innocenti e condivide tali informazioni con varie agenzie senza la benché minima supervisione. È il genere di cosa che ci si aspetterebbe dall'ex Unione Sovietica o dalla Germania dell'Est o dalla Cina. E non ci rende più sicuri contro il terrorismo.

Articoli a riguardo:

<http://news.yahoo.com/s/ap_travel/20061208/ap_tr_ge/travel_brief_travel_er_screening> oppure <<http://tinyurl.com/yygbda>>
<<http://www.washingtonpost.com/wp-dyn/content/article/2006/11/02/AR2006110201810.html>> oppure <<http://tinyurl.com/y192on>>
<<http://www.ledger-enquirer.com/mld/ledgerenquirer/news/local/16196947.htm>> oppure <<http://tinyurl.com/y7lbnp>>

La pubblicazione del Registro Federale:

<<http://edocket.access.gpo.gov/2006/06-9026.htm>>

I commenti dei gruppi sostenitori delle libertà civili:

<http://www.epic.org/privacy/pdf/ats_comments.pdf>
<http://www.eff.org/Privacy/ats/ats_comments.pdf>
<<http://www.aclu.org/privacy/gen/27593leg20061201.html>>
<<http://www.epic.org/privacy/travel/ats/default.html>>
<<http://www.epic.org/privacy/surveillance/spotlight/1006/default.html>>

Il profiling antiterroristico automatizzato:

<<http://www.schneier.com/essay-108.html>>
<<http://www.schneier.com/essay-115.html>>
<http://www.newyorker.com/fact/content/articles/060206fa_fact>
<http://www.cato.org/pub_display.php?pub_id=6784>

No-fly list:

<<http://alternet.org/story/42646/>>
<<http://www.aclu.org/safefree/resources/17468res20040406.html>>

Secure Flight:

http://www.schneier.com/blog/archives/2005/07/secure_flight.html

Total Information Awareness:

<http://www.epic.org/privacy/profiling/tia/>

Il sistema ATS potrebbe essere illegale:

<http://hasbrouck.org/IDP/IDP-ATS-comments.pdf>

<http://www.washingtonpost.com/wp-dyn/content/article/2006/12/08/AR2006120801833.html> oppure <http://tinyurl.com/u2j9s>

<http://www.wired.com/news/technology/0,72250-0.html>

<http://www.ledger-enquirer.com/mld/ledgerenquirer/news/local/16196947.htm>

<http://leahy.senate.gov/press/200612/120606.html>

Questo articolo, senza i link, è stato pubblicato in Forbes.

http://www.forbes.com/forbes/2007/0108/032_print.html

Forbes ha anche pubblicato una confutazione di William Baldwin, anche se non sembra confutare nessuno dei punti principali. "Ecco una strana divisione del lavoro: un consulente di dati aziendali vuole una maggiore apertura, mentre un giornalista è a favore di una maggiore segretezza". È strana solo per chi non comprende la sicurezza.

<http://www.forbes.com/forbes/2007/0108/014.html>

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

Telecamere di sorveglianza filmano un assassino a sangue freddo

Sto scrivendo un lungo saggio sulla psicologia della sicurezza. Uno degli argomenti trattati è la "disponibilità euristica", la quale sostanzialmente afferma che il cervello umano tende a valutare la frequenza di una classe di eventi basandosi sulla facilità di richiamare alla mente un'istanza di tale classe. Spiega perché le persone tendono a preoccuparsi dei rischi trattati dai media, o perché si ha paura di volare ma non di guidare un'auto.

Uno degli effetti di tale euristica è che la gente viene persuasa più da un esempio reale che dalle statistiche. Queste ultime possono rivelarsi più utili, ma il primo è più semplice da ricordare.

Questo è il contesto in cui voglio che leggiate la storia, piuttosto scioccante, di un assassino a sangue freddo filmato da telecamere di sorveglianza cittadine.

"Gli agenti federali hanno mostrato a Peterman le registrazioni di quella mattina. Una telecamera ha ripreso McDermott, 48 anni, mentre scendeva dall'autobus. Un uomo con indosso una giacca leggera e pantaloni scuri è sceso dal medesimo autobus e l'ha seguita a pochi passi di distanza.

"Un'altra telecamera li ha ripresi mentre giravano l'angolo. McDermott pare non si sia accorta dell'uomo che la seguiva. A metà strada nell'isolato, l'uomo ha improvvisamente sollevato il braccio e ha sparato alla donna, un solo colpo alla nuca.

" 'Non è la prima volta che vedo sparatorie filmate da telecamere', ha

detto Peterman, 'ma la subitaneità dell'atto e la totale assenza di un motivo sono state spaventose'. "

Posso scrivere fiumi di parole sull'inefficacia delle telecamere di sicurezza, parlare di compromessi e di sistemi migliori per spendere denaro. Posso citare statistiche, opinioni di esperti, e tutto quel che voglio. Ma, se utilizzate in modo appropriato, storie come questa saranno in grado di smuovere l'opinione pubblica molto più di qualsiasi cosa io possa fare.

<http://abcnews.go.com/2020/story?id=2755037>

** *** *****

Le ristampe di Crypto-Gram

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

<http://www.schneier.com/crypto-gram-back.html>. Quella che segue è una selezione di articoli apparsi in questo mese gli anni scorsi (le corrispondenti traduzioni in italiano le potete trovare all' indirizzo <http://www.cryptogram.it/crypto-gram.html>, ndt).

Anonimato e responsabilità:

<http://www.schneier.com/crypto-gram-0601.html#1>

Le intercettazioni illegali di Bush e della NSA:

<http://www.schneier.com/crypto-gram-0601.html#12>

La minaccia per la sicurezza che deriva da un potere presidenziale non controllato:

<http://www.schneier.com/crypto-gram-0601.html#13>

Prendere le impronte digitali agli studenti:

<http://www.schneier.com/crypto-gram-0501.html#1>

La Guerra Cibernetica:

<http://www.schneier.com/crypto-gram-0501.html#10>

Dirottare aerei e Servizi Segreti nazionali:

<http://www.schneier.com/crypto-gram-0401.html#11>

Prendere le impronte digitali agli stranieri:

<http://www.schneier.com/crypto-gram-0401.html#3>

I livelli di minaccia terroristica codificati a colori:

<http://www.schneier.com/crypto-gram-0401.html#1>

L'esercito e la Guerra Cibernetica

<http://www.schneier.com/crypto-gram-0301.html#1>

Una Underwriters Laboratories in versione cibernetica?

<http://www.schneier.com/crypto-gram-0101.html#1>

Code signing:

<http://www.schneier.com/crypto-gram-0101.html#10>

Block ciphers e stream ciphers:

<http://www.schneier.com/crypto-gram-0001.html#BlockandStreamCiphers>

** *** *****

Intercettazioni uditive

Nell'era dell'informazione, la sorveglianza non è solo affare della polizia. Anche i commercianti vogliono osservarvi: che cosa fate, dove andate, che cosa acquistate. Integrated Media Measurement, Inc. vuole sapere che cosa guardate e che cosa ascoltate ovunque vi troviate.

Tale obiettivo viene ottenuto capovolgendo il sistema di rilevazione degli indici di ascolto televisivi tradizionale. Invece di un sistema tipo Nielsen, che osserva i singoli apparecchi televisivi cercando di stabilire in quanti stanno davanti al televisore, IMMI osserva i singoli individui e cerca di stabilire che cosa stanno guardando (o ascoltando). Per fare ciò, l'azienda si serve di telefoni cellulari speciali che si mettono automaticamente in ascolto di quel che sta accadendo nella stanza in cui si trovano:

"Il telefono IMMI campiona casualmente 10 secondi di audio ambientale ogni 30 secondi. Questi campioni vengono ridotti a firme digitali, inviate di continuo ai server IMMI.

"Inoltre IMMI traccia tutte le sorgenti media che stanno trasmettendo in una determinata area (DMA). Per identificare i media, IMMI confronta le firme audio caricate online che sono state elaborate dai telefoni con le firme audio elaborate dai server IMMI che monitorano le trasmissioni radio e TV. IMMI mantiene poi tutta una serie di file di contenuti messi a disposizione dai clienti, come spot pubblicitari, promo, film e canzoni.

"Confrontando le firme, IMMI accoppia le trasmissioni con gli individui che le stanno guardando/ascoltando. Il procedimento richiede solo alcuni secondi.

"I membri del panel di consumatori possono a volte vedere o ascoltare un programma in differita, mediante l'utilizzo di radio satellitari, DVR, videoregistratori o TiVo. IMMI cattura questi ascolti con una funzione 'look-back' che rileva quando un membro del panel di consumatori sta guardando un programma al di fuori dell'orario normale di messa in onda, e indaga indietro nel tempo (circa due settimane) per stabilire di che programma si tratta".

Questi telefoni cellulari vengono forniti a soggetti di prova, a cui viene offerto un servizio gratuito in cambio del completo abbandono della propria privacy.

L'azienda sostiene che la propria tecnologia non può venire utilizzata per intercettare conversazioni all'interno di una stanza o conversazioni telefoniche. Ma le modifiche che ha apportato ai propri cellulari dimostrano che è possibile alterare i telefoni in altri modi. È possibile installare un altro software di intercettazione su cellulari

nuovi? Una cosa del genere può essere fatta all'insaputa e contro la volontà del proprietario? Qui il potenziale per commettere abusi è elevatissimo, magari non da parte di IMMI, ma certamente da terzi.

Ricordate, le minacce contro la privacy nell'era dell'informazione non giungono solo da parte dei governi, ma anche dall'industria privata. E la vera minaccia è l'alleanza fra i due.

[<http://www.immi.com/>](http://www.immi.com/)

[<http://www.immi.com/dataClctn.html>](http://www.immi.com/dataClctn.html)

[<http://www.immi.com/privacy.html>](http://www.immi.com/privacy.html)

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

Tener traccia delle automobili tramite i loro pneumatici

Ai pneumatici delle automobili ora vengono aggiunti dei trasmettitori RFID: scommetto che è possibile tener traccia dei veicoli mediante questo accorgimento, proprio come è possibile tener traccia di chi fa jogging tramite le sue scarpe da ginnastica.

Come ho già detto, le persone che progettano questi sistemi "non hanno minimamente pensato alla sicurezza né alla privacy. A meno di non emanare una legge ad ampio spettro che obblighi le aziende ad aggiungere un livello di sicurezza a questo genere di sistemi, le compagnie continueranno a produrre dispositivi che riducono la nostra privacy attraverso nuove tecnologie. Non lo fanno di proposito, o perché sono in malafede, semplicemente perché è più facile ignorare l'esternalità che preoccuparsi di essa".

[<http://www.schrader-bridgeport.com/index.cfm?location_id=4816>](http://www.schrader-bridgeport.com/index.cfm?location_id=4816)

Seguire le tracce di qualcuno attraverso le sue scarpe da ginnastica:

[<http://www.schneier.com/blog/archives/2006/12/tracking_people.html>](http://www.schneier.com/blog/archives/2006/12/tracking_people.html)

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

Accordare una licenza ai barcaioli

La Guardia Costiera statunitense sta pensando di accordare licenze ai barcaioli. Se ne sta parlando in termini di misura antiterrorismo, con la solita incoerenza:

"Gli Stati Uniti hanno già subito atti terroristici mediante l'uso di piccole imbarcazioni civili, seppur oltremare: nel 2000 dei bombaroli suicidi nel porto di Aden, nello Yemen, hanno impiegato un'imbarcazione gonfiabile per farsi saltare in aria nei pressi del cacciatorpediniere USS Cole della Marina degli Stati Uniti, uccidendo 17 marinai e ferendone altri 39.

"Gli esperti di terrorismo indicano altri sistemi con cui delle piccole imbarcazioni potrebbero servire durante un attacco: per esempio, un veloce motoscafo potrebbe depositare dei sabotatori alle condutture di sbocco di una centrale nucleare, o dei dirottatori a bordo di una nave

da crociera. In uno dei peggiori scenari, dei bombaroli suicidi in un porto affollato potrebbero servirsi di piccole imbarcazioni per far saltare una cisterna contenente gas naturale liquefatto ultravolatile, provocando una potentissima esplosione che potrebbe uccidere migliaia di persone”.

E a che cosa esattamente servirebbe concedere una licenza alle imbarcazioni?

Vi sono tante ragioni più che buone per accordare licenze per imbarcazioni e barcaioli, come ve ne sono altrettante per concedere patenti di guida e immatricolare veicoli. Ma l'antiterrorismo non è una di queste.

<http://www.stateline.org/live/details/story?contentId=165344>

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

Un centro commerciale Wal-Mart rimane aperto durante un allarme bomba

Un centro commerciale Wal-Mart in Mitchell, South Dakota riceve un allarme bomba. La direzione decide di non far evacuare il centro mentre la polizia lo setaccia in cerca dell'ordigno. Presumibilmente, i direttori hanno deciso che la perdita di guadagni dovuta a un'evacuazione non valeva la sicurezza aggiuntiva dell'evacuazione:

“Durante la ricerca della bomba (quasi due ore), i responsabili del Wal-Mart hanno scelto di non far evacuare l'affollato store anche se le forze dell'ordine avevano consigliato loro di farlo. I responsabili del Wal-Mart hanno detto che la chiamata era uno scherzo e non una vera minaccia”.

Credo che questo sia un buon segno. Dimostra che le persone stanno iniziando a pensare razionalmente in merito ai compromessi di sicurezza, e che non si lasciano terrorizzare.

Però occorre ricordare che i compromessi di sicurezza si basano su un'agenda di priorità. Dal punto di vista dei direttori del Wal-Mart, i profitti del centro commerciale sono più importanti di ogni altra cosa; molti dei rischi dell'allarme bomba sono esternalità.

Ovviamente, l'agenda degli impiegati del centro commerciale è ben diversa: non vi è alcun vantaggio nel rimanere aperti, solo un inconveniente dovuto al rischio che si viene a creare. E non hanno gradito la decisione presa dai direttori.

Ecco la dichiarazione di un impiegato, contenuta nell'articolo:

“Manca pochissimo a Natale. C'era gente dappertutto”, ha detto, “Secondo me hanno messo in pericolo la comunità, i clienti e i colleghi. Hanno messo i guadagni davanti all'incolumità della gente”.

<http://argusleader.com/apps/pbcs.dll/article?AID=/20061227/NEWS/61227028/-1/UPDATES> oppure <http://tinyurl.com/y337kz>

** *** *****

News

La vicenda allarmante di una persona a cui è stato comunicato da parte della sua banca che non è più il benvenuto come cliente, poiché il computer della banca ha notato un deposito che non era "normale". Questo è ciò che avviene quando si usa un profiling basato sui computer. Aspettiamoci altre storie come questa, visto che sempre più spesso sono le macchine a decidere chi è normale e chi non lo è.
<<http://www.lightbluetouchpaper.org/2006/09/26/closing-in-on-suspicious-transactions/>> oppure <<http://tinyurl.com/jkf2n>>

Le previsioni AccuTerror di Bill Maher. Divertente.
<<http://www.youtube.com/watch?v=Dmnpph86B8U>>

Un buon articolo sulla sicurezza aeroportuale e sulla TSA. Contiene ottime citazioni di Matt Blaze e del sottoscritto.
<<http://www.nytimes.com/2006/12/17/business/yourmoney/17digi.html?ex=1324011600&en=db7ab439c0c47253&ei=5090&partner=rssuserland&emc=rss>> oppure <<http://tinyurl.com/w24s2>>

Fra l'altro, molte persone mi rimproverano costantemente di lamentarmi della sicurezza aerea senza mai offrire soluzioni. In genere rimando queste persone alla lettura degli ultimi due paragrafi di quest'articolo:
<<http://www.schneier.com/essay-096.html>>

Clonare passaporti RFID in cinque minuti:
<http://news.bbc.co.uk/2/hi/programmes/click_online/6182207.stm>

Suggerimento di sicurezza aeroportuale: non mettete il vostro bambino nella macchina a raggi X.
<<http://www.latimes.com/news/local/la-me-baby20dec20,0,6460373.story>>

Ecco una persona che scavalca una recinzione al Raleigh-Durham Airport, sale a bordo di un aereo delle linee Delta e se la spassa per qualche ora. La parte migliore dell'articolo: "È incredibile come sia impossibile portare 3,5 onces di dentifricio su un aereo", ha detto, "e al tempo stesso un individuo qualunque possa intrufolarsi su un aereo e farsi un pisolino". Appunto. Stiamo spendendo milioni di dollari per migliorare lo screening dei passeggeri e ignoriamo gli altri metodi, meno sicuri, per imbarcarsi sugli aerei. È pura idiozia, ecco quel che è.
<<http://www.newsobserver.com/102/story/523482.html>>

Il sito Web della TSA è un luogo affascinante per passare il tempo navigando. Hanno regole per maneggiare le scimmie: "Gli operatori della TSA sono stati addestrati a non toccare la scimmia durante la procedura di screening".
<http://www.tsa.gov/travelers/airtravel/assistant/editorial_1056.shtm>
Ed è proibito portare i globi di neve nel bagaglio a mano: "I globi di neve, a prescindere dalle dimensioni o dalla quantità di liquido al loro interno, anche se accompagnati da relativa documentazione, sono vietati nel bagaglio a mano. Si prega di spedire questi oggetti o di metterli nel bagaglio imbarcato".
<<http://www.tsa.gov/travelers/airtravel/prohibited/permitted-prohibited-items.shtm>> oppure <<http://tinyurl.com/ptxdw>>

Mi faccio beffe della sicurezza aerea nel "New York Times".

<http://www.nytimes.com/2007/01/02/business/02road.html?ex=1325394000&en=48df7bb5fe411ec9&ei=5090&partner=rssuserland&emc=rss> oppure
<http://tinyurl.com/ybc8aa>

"Family Guy" sulla sicurezza aeroportuale. È impressionante il fatto che fu trasmesso prima dell'11 settembre. Ora la satira è ancora migliore.

<http://www.youtube.com/watch?v=JireQ-si43Q>

Ottimo articolo di Matt Blaze sull'architettura e la sicurezza negli aeroporti:

http://www.crypto.com/blog/airport_architecture/

Il Privacy Office del Dipartimento per la Sicurezza Nazionale ha rilasciato un rapporto sulle problematiche di privacy di Secure Flight, il nuovo programma per lo screening dei passeggeri delle linee aeree. Non è molto buono, per questo il governo ha cercato di farlo passare inosservato rilasciandolo al pubblico il venerdì prima di Natale.

<http://www.dhs.gov/xlibrary/assets/privacy/privacy-secure-flight-122006.pdf> oppure <http://tinyurl.com/yx6g5o>

http://www.schneier.com/blog/archives/2007/01/secure_flight_p_1.html

Ho parlato molte volte di Secure Flight.

http://www.schneier.com/blog/archives/2005/07/secure_flight.html

http://www.schneier.com/blog/archives/2005/09/secure_flight_n_1.html

Il Privacy Office del Dipartimento per la Sicurezza Nazionale ha inoltre rilasciato un rapporto su MATRIX (Multistate Anti-Terrorism Information Exchange). MATRIX è un programma (ora non più in vigore) di data mining e data sharing fra le agenzie delle forze dell'ordine a livello federale, statale e locale, uno dei tanti programmi di data mining governativi (il più famoso è TIA, Total Information Awareness, e il più recente è Tangram). Il rapporto è breve e molto critico per quanto riguarda la totale mancanza di attenzione alla privacy e la mancanza di trasparenza di tale programma. Ecco perché, anche in questo caso, è stato rilasciato al pubblico poco prima di Natale, rimanendo sommerso dai media.

<http://www.dhs.gov/xlibrary/assets/privacy/privacy-matrix-122006.pdf>

Maggiori informazioni su MATRIX:

<http://www.aclu.org/privacy/spying/15701res20050308.html>

Maggiori informazioni sul data mining:

http://www.epic.org/privacy/profiling/gao_dm_rpt.pdf

http://www.schneier.com/blog/archives/2006/03/data_mining_for.html

<http://www.epic.org/privacy/profiling/tia/>

http://www.schneier.com/blog/archives/2006/10/total_informati.html

OneDOJ è un ennesimo gigantesco database governativo, ideato per raccogliere tutti i database delle forze dell'ordine federali:

http://www.washingtonpost.com/wp-dyn/content/article/2006/12/25/AR2006122500483_pf.html oppure <http://tinyurl.com/v4jkq>

Inserire a computer tutto questo materiale è una buona idea, ma ogni nuovo sistema necessita di un'intrinseca tutela della privacy. Occorre assicurarsi: 1) che sia possibile correggere informazioni imprecise, 2) che i dati vengano cancellati una volta che non siano più necessari, soprattutto informazioni investigative su persone che si sono rivelate innocenti, e 3) che siano implementate delle protezioni contro l'abuso dei dati, sia da parte di persone autorizzate ad accedervi, sia da parte di persone che agiscono in maniera non ufficiale o fraudolenta. Nella

fretta di inserire a computer tutti questi registri, si stanno ignorando queste salvaguardie e si stanno costruendo sistemi che ci renderanno tutti meno sicuri.

US-VISIT, il programma per tenere efficacemente traccia delle persone che entrano ed escono dagli Stati Uniti, sta avendo ogni genere di problema. Ed è stato accantonato, per ora temporaneamente, e forse definitivamente. Mi piace il sentimento di compromesso che traspare da questa citazione di un articolo: "Vi sono molte buone idee e molte cose che renderebbero il paese più sicuro. Ma quando bisogna fermarsi e confrontare tutte queste buone idee che si sono venute sviluppando, e si ha un budget limitato, è necessario effettuare scelte molto più difficili". A mio avviso il programma verrà completamente terminato dal Congresso nel corso del 2007.

<http://www.navyseals.com/community/articles/article.cfm?id=10348>

<http://www.fcw.com/article97142-12-18-06-Web>

<http://www.rfidjournal.com/article/articleview/2915/1/1/>

<http://www.newsday.com/news/opinion/ny-vpvis265028876dec26,0,5078413.st>
ory?coll=ny-editorials-headlines> oppure <http://tinyurl.com/y6kyyn>

Ulteriori informazioni su US-VISIT:

<http://www.schneier.com/essay-072.html>

<http://www.epic.org/privacy/surveillance/spotlight/0705>

http://www.dhs.gov/xtrvlsec/programs/content_multi_image_0006.shtm

http://www.schneier.com/blog/archives/2006/01/the_failure_of_1.html

È altresì molto improbabile che il nuovo Congresso (saggiamente, a mio giudizio) stanzi i finanziamenti per la recinzione di 700 miglia lungo il confine con il Messico.

http://www.house.gov/hunter/news_prior_2006/fence.amendment.html

Spero che il Congresso prenda in esame i fallimenti di sicurezza e le eccedenze dei costi della Guardia Costiera.

<http://www.wirednewyork.com/forum/showthread.php?t=11761>

Si noti che l'articolo parla dei gravi scontri fra Guardia Costiera e FBI. Sarebbe bello che il Congresso dedicasse un po' di tempo per risolvere questo problema, che è decisamente serio.

Il governo degli Stati Uniti ha indetto una competizione aperta per selezionare un produttore che implementi la crittografia dei dischi rigidi di tutti i computer portatili del governo. Criptare tutti i dati è certamente esagerato, ma è molto più semplice che decidere che cosa criptare e cosa no. E apprezzo davvero che vi sia una competizione aperta per decidere quale programma di crittografia impiegare. È di sicuro una competizione che presenta una posta molto alta in gioco per i vari produttori, ma questo non fa altro che migliorare la sicurezza di tutti i prodotti. È da molto tempo che sostengo che una delle cose migliori che può fare il governo per aumentare la sicurezza informatica è quella di utilizzare il suo enorme potere di acquisto per spingere i produttori a migliorare la loro sicurezza. Mi aspetto che il vincitore venda moltissimo al di fuori del contratto governativo, e che i perdenti colgano l'occasione per correggere i difetti dei loro prodotti, così da far meglio la prossima volta.

http://www.schneier.com/blog/archives/2007/01/us_government_t.html

Mi chiedo se la NSA sia coinvolta nel processo di valutazione e, in caso affermativo, se le sue analisi verranno rese pubbliche.

War on Terror: il gioco da tavolo:

<http://www.waronterrortheboardgame.com/thegame/>

"A Cost Analysis of Windows Vista Content Protection" [Un'analisi dei costi della protezione dei contenuti in Windows Vista] di Peter Gutman è una lettura affascinante.

http://www.schneier.com/blog/archives/2006/12/a_cost_analysis.html

http://www.cs.auckland.ac.nz/~pgut001/pubs/vista_cost.txt

<http://www.miraesoft.com/karel/2006/12/25/cost-analysis-of-windows-vista-content-protection/> oppure <http://tinyurl.com/yxdqry>

Il Direttore delle Comunicazioni del membro del congresso Denny Rehberg, del Montana, ha invitato degli hacker a introdursi nel sistema informatico della sua università per cambiargli i voti (così da apparire migliori quando si fosse messo in lizza per una posizione, suppongo). Gli hacker, invece, hanno pubblicato l'intero scambio di email. Molto divertente.

<http://www.attrition.org/postal/z/033/0871.html>

<http://www.networkworld.com/community/?q=node/9999>

Tutti sanno che scrivere la propria password sul monitor è pessima sicurezza. È così difficile capire che attaccare il proprio token SecurID al computer è altrettanto stupido?

<http://thedailywtf.com/forums/thread/107695.aspx>

AACS (Advanced Access Content System), il sistema di protezione anticopia utilizzato nei Blu-Ray e nei HD DVD, potrebbe essere stato craccato... più o meno.

<http://forum.doom9.org/showthread.php?p=924730#post924730>

<http://www.edn.com/blog/400000040/post/1240006124.html>

Eccellente analisi:

<http://www.freedom-to-tinker.com/?p=1104>

<http://www.freedom-to-tinker.com/?p=1106>

<http://www.freedom-to-tinker.com/?p=1107>

<http://www.freedom-to-tinker.com/?p=1108>

Una recensione di "Kim", di Rudyard Kipling: "Kipling introduceva un gran quantitativo di informazioni e di concetti nelle sue storie, e in 'Kim' troviamo il Grande Gioco di spionaggio. Nelle prime venti pagine abbiamo: autenticazione mediante un oggetto posseduto, denial of service, sostituzione di persona, segretezza, montatura, autorizzazione basata sul ruolo (con autenticazione ad hoc mediante qualcosa che si conosce), intercettazione e fiducia basata sull'integrità dei dati. Più avanti troviamo: elaborazione di un piano di emergenza contro il furto e crittografia con cambiamenti di chiave".

<http://catless.ncl.ac.uk/Risks/24.49.html#subj12>

Il libro non è più soggetto a copyright. Leggetelo qui:

<http://whitewolf.newcastle.edu.au/words/authors/K/KiplingRudyard/prose/Kim/index.html> oppure <http://tinyurl.com/tpexg>

<http://kipling.thefreelibrary.com/Kim>

<http://www.readprint.com/work-935/Rudyard-Kipling>

In Scozia vi è una proposta (che ci crediate o no) di emettere documenti di identificazione per i bambini per evitare prepotenze. Pare che i bulli si appropriino delle tessere mensa degli altri ragazzini, e che fermando questa tendenza grazie a documenti di identità le prepotenze cesseranno magicamente di esistere. Sono d'accordo con quanto afferma il parlamentare Patrick Harvie alla fine dell'articolo.

<http://news.bbc.co.uk/1/hi/scotland/6210977.stm>

Un giudice della Florida ha stabilito che il candidato perdente non ha alcun diritto di esaminare il codice sorgente delle macchine per il voto elettronico che hanno determinato il vincitore in una gara elettorale per il Congresso.

<<http://www.heraldtribune.com/apps/pbcs.dll/article?AID=/20061229/BREAKING/61229007>> oppure <<http://tinyurl.com/ylydxx>>
<<http://electionlawblog.org/archives/ess-pdf.pdf>>

Nel frattempo a Ciber Inc., il laboratorio che ha verificato la maggior parte delle macchine per il voto utilizzate a livello nazionale, è stato temporaneamente proibito di approvare le macchine perché si è scoperto che non stava seguendo le procedure di verifica stabilite e che non è stato in grado di fornire adeguata documentazione che attestasse l'esecuzione di tali verifiche.

<<http://www.libertypost.org/cgi-bin/readart.cgi?ArtNum=171610>>

Questa serratura a combinazione molecolare è impressionante:

<<http://www.engadget.com/2006/12/29/chemists-craft-molecular-keypad-lock/>> oppure <<http://tinyurl.com/y94uau>>

Il New York Times ha un'entrata di blog che parla di come sia facile mettersi in ascolto in una sessione Wi-Fi aperta. È bello vedere come questo argomento stia ottenendo l'attenzione del pubblico.

<<http://pogue.blogs.nytimes.com/2007/01/04/04pogue-email/>>

Come recuperare numeri da immagini sfocate:

<<http://dheera.net/projects/blur.php>>
<<http://reddit.com/info/xaae/comments/cxbgy>>

Ecco un'idea stupida: allarmi terrorismo del MI5 via email:

<http://news.bbc.co.uk/2/hi/uk_news/6242883.stm>

Ho già trattato l'argomento allarmi terrorismo nel Regno Unito:

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

Un articolo del 1933 sulla tecnologia per il gioco d'azzardo sleale. In ogni generazione, i criminali sono quasi sempre all'avanguardia nell'applicare nuove tecnologie per rubare.

<<http://blog.modernmechanix.com/2007/01/09/strange-inventions-used-by-croked-gamblers/>> oppure <<http://tinyurl.com/yzzchz>>

Stanno rubando le identità dei nostri bambini! È questo il genere di cose che spinge i legislatori ad agire? Dopotutto, dobbiamo proteggere i nostri bambini.

<http://www.bankrate.com/nltrack/news/debt/20070103_child_identity_theft_a1.asp> oppure <<http://tinyurl.com/vagyq>>

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

La NSA aiuta Microsoft con Windows Vista

La NSA ha "aiutato" Microsoft con Windows Vista. Ovviamente non hanno divulgato che cosa hanno fatto, ma fonti all'interno di Microsoft mi hanno detto che non è stato niente più che semplice assistenza nei test di verifica.

Ma ho dei sospetti.

Si chiama "equities issue", questione di equità. Sostanzialmente la NSA ha due ruoli: intercettare le cose altrui e proteggere le nostre. Quando entrambe le parti utilizzano la stessa cosa, Windows Vista per esempio, l'agenzia deve decidere se sfruttare le vulnerabilità per intercettare le cose altrui o chiudere le medesime vulnerabilità per proteggere le nostre cose. Nella sua partnership con Microsoft può aver scelto di agire in uno qualsiasi dei due modi: introdurre deliberatamente delle vulnerabilità che solo essa può sfruttare, o rendere il sistema operativo più robusto per proteggere i propri interessi.

Qualche anno fa sarei stato disposto a credere che la NSA avesse capito che siamo tutti più al sicuro mediante computer e reti più sicure, ma nel clima di intercettazione globale successivo all'11 settembre non ho fiducia che la NSA decida di comportarsi correttamente.

<http://www.washingtonpost.com/wp-dyn/content/article/2007/01/08/AR2007010801352.html> oppure <http://tinyurl.com/ycqv9f>

Un'altra opinione:

<http://www.computerworld.com/blogs/node/4330>

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

Il sistema anti-phishing di Microsoft e le piccole imprese

Microsoft ha inserito un nuovo servizio anti-phishing in Internet Explorer 7: quando i visitatori raggiungono siti precedentemente verificati e dichiarati legittimi, il campo indirizzo del browser diventerà verde e mostrerà l'identità del proprietario del sito. Fin qui tutto bene. Ma il servizio è disponibile solo alle aziende: non alle imprese individuali, alle partnership o ai privati.

Naturalmente, se il campo indirizzo non diventa verde, non significa che il tal sito sia malevolo. Sarà bianco, il che indica "nessuna informazione". Vi sono anche degli indicatori giallo e rosso, che corrispondono a "sospetto" e a "sito fraudolento conosciuto". Ma le piccole imprese temono che i clienti abbiano paura a comprare da siti non verdi.

Questo è possibile, ma è più probabile che gli utenti si rendano conto dell'inaffidabilità del marcatore e inizieranno a ignorarlo.

Un qualsiasi sistema di white list come questo è suscettibile di due tipi di errore: i falsi positivi, ovvero i phisher ottengono il marcatore verde, e i falsi negativi, ovvero i commercianti onesti e legittimi non ottengono il verde. Tutti i sistemi di questo tipo devono affrontare entrambe le situazioni in modo efficace.

http://online.wsj.com/public/article/SB116649577602354120-5U4Afb0JPeyiOy1H_j3fVTUmfG8_20071218.html?mod=rss_free oppure <http://tinyurl.com/y7ezyr>

"Phinding Phish: An Evaluation of Anti-Phishing Toolbars" [Una valutazione delle barre strumenti anti-phishing] di L. Cranor, S. Egleman, J. Hong e Y. Zhang.

<http://www.cylab.cmu.edu/files/cmucylab06018.pdf>

** *** *****

Le sviste del Dipartimento della Motorizzazione della Virginia

Sono state concesse patenti di guida dello stato della Virginia a due uomini anche se i due individui erano visibilmente camuffati quando il Dipartimento della Motorizzazione ha scattato le foto per i documenti. I video dell'accaduto sono online.

Il Dipartimento della Motorizzazione della Virginia ha ora ordinato che i due uomini si ripresentino affinché vengano scattate delle foto regolari.

Non ho mai pensato di dover dire una cosa del genere, ma mi trovo completamente d'accordo con quanto ha sostenuto Michelle Malkin sulla vicenda:

"Questi tizi hanno fatto un grosso favore al Dipartimento della Motorizzazione della Virginia e all'intera nazione. Molti di noi hanno cercato di dimostrare quanto queste agenzie e la nostra sicurezza nazionale rimangano risibili anche dopo l'11 settembre, specialmente l'emissione di patenti di guida (fu il Dipartimento della Motorizzazione della Virginia che concesse documenti di identità con foto a molti dei dirottatori dell'11 settembre che furono aiutati da immigrati clandestini).

"Ma ben poche dissertazioni e analisi di condotta sono in grado di centrare il messaggio più efficacemente di questi due dannati video".

Onestamente non so se Malkin si renda conto che REAL ID non risolverà questo genere di problemi, però. Né risolverà il problema di persone che ottengono documenti d'identità legittimi con i nomi di coloro ai quali hanno sottratto l'identità, o di veri documenti d'identità emessi sotto falsi nominativi da impiegati corrotti del Dipartimento della Motorizzazione.

I video:

http://www.youtube.com/watch?v=j0Ff_KB3lI

<http://www.youtube.com/watch?v=owvO640DwA>

Malkin:

<http://michellemalkin.com/archives/006589.htm>

REAL-ID:

http://www.schneier.com/blog/archives/2005/05/real_id.html

** *** *****

Ancora sul codice di Unabomber

Lo scorso mese ho parlato della crittografia a carta e matita di Ted Kaczynski. Pare che abbia inventato il suo proprio cipher, che la

polizia non avrebbe potuto codificare se non avesse trovato una descrizione del codice fra le sue carte.

Il link che ho trovato proveniva da KPIX, una società affiliata alla CBS nella zona di San Francisco. Tempo dopo averlo scritto, sono stato contattato dalla stazione televisiva e mi è stato chiesto di commentare altri pezzi della crittografia di Unabomber per una storia che stavano realizzando (il video è online).

Vi erano cinque nuove pagine del codice di Unabomber di cui avevo parlato (tutte disponibili sul sito della CBS5). Tutte e cinque le pagine mi furono presentate come scritte da Unabomber, ma mi sembra piuttosto evidente che le pagine 4 e 5 non rappresentano la chiave di Kaczynski; sono note scritte da un criptoanalista che ha cercato di decodificare il codice di Unabomber.

In ogni caso, è tutto molto affascinante.

http://cbs5.com/investigates/local_story_363002905.html

Il mio intervento del mese scorso:

http://www.schneier.com/blog/archives/2006/12/unabombers_code.html

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

Le news di BT Counterpane

Schneier parteciperà a una tavola rotonda su questioni economiche e di sicurezza nel corso di un OECD Security Workshop a Washington DC il 31 gennaio.

Schneier parlerà della "Psicologia della Sicurezza" [The Psychology of Security] alla RSA Conference a San Francisco il 6 febbraio:

<http://www.rsaconference.com/2007/US/>

Schneier intervorrà al Linux World Open Solutions Summit a New York il 14 febbraio:

<http://www.linuxworldsummit.com/live/14/>

Schneier intervorrà alla ottava edizione della Annual Privacy and Security Conference a Victoria, BC, il 15 febbraio:

<http://www.rebootconference.com/privacy2007/about.php>

Il profilo di Schneier secondo DarkReading:

http://www.darkreading.com/document.asp?doc_id=114230&WT.svl=news1_1

Lo "Arizona Star" ha pubblicato un editoriale di opinione di Schneier sulla sorveglianza all'ingrosso:

<http://www.azstarnet.com/allheadlines/164048.php>

L'aggancio di cronaca che ho utilizzato è stato un articolo sulla polizia che sta collaudando uno scanner di targhe automobilistiche montato sui propri veicoli. Purtroppo ho indicato erroneamente un altro dipartimento di polizia. Si tratta dell'Arizona State Police, non della Tucson Police.

<http://www.azstarnet.com/allheadlines/144548>

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

Radiotrasmittitori nascosti nelle monete canadesi

Una vicenda piuttosto bizzarra:

"Almeno tre fornitori statunitensi in visita nel Canada si sono trovati nelle tasche delle monete canadesi contenenti piccolissimi radiotrasmittitori, ha dichiarato una branca del Dipartimento della Difesa USA.

"Gli esperti di sicurezza ritengono che tali dispositivi miniaturizzati potrebbero essere usati per tracciare i movimenti di impiegati dell'industria della difesa che trattano tecnologia militare segreta".

Suona davvero poco plausibile. Vi sono moltissime altre maniere di tener traccia di qualcuno che non quella di dargli un oggetto che darà a qualcun altro la prossima volta che si prende un caffè. Si può usare il suo cellulare, per esempio.

E poco dopo, ecco un aggiornamento della vicenda:

"Il rapporto secondo cui alcune monete canadesi sono state compromesse da trasmettitori-spia segretamente piazzati al loro interno è tutta un'esagerazione, secondo un ufficiale statunitense a conoscenza del caso.

"Non vi è alcuna storia qui", ha dichiarato a The Globe e al Mail l'ufficiale, che ha chiesto di rimanere anonimo.

"Ha affermato che, sebbene alcune monete canadesi dall'aspetto curioso abbiano brevemente destato sospetti negli Stati Uniti, tali paure si sono rivelate infondate: 'Non abbiamo alcuna prova a indicare che tali monete (o qualsiasi cosa sia ad esse collegato) rappresentino un rischio o una minaccia'".

Scegliete voi a cosa credere. O la storia originale è stata esagerata, oppure chi ne è coinvolto sta cercando di depistare le notizie per coprire le proprie tracce. Non abbiamo molti fatti a disposizione, qui.

http://ca.news.yahoo.com/s/capress/spy_money

<http://www.theglobeandmail.com/servlet/story/RTGAM.20070110.wspycoin0110/BNStory/National/home> oppure <http://tinyurl.com/ym7zpb>

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

Scegliere password sicure

Da quando ho parlato delle 34.000 password di MySpace che ho analizzato, molte persone mi hanno scritto chiedendomi come scegliere delle password sicure. Nel corso degli anni sono state scritte molte cose sull'argomento, ma la maggior parte di esse pare basarsi più su suggerimenti aneddotici che non su prove analitiche vere e proprie. Quel che segue sono consigli seri e provati.

L'attacco contro il quale fondo la mia valutazione è un attacco password-guessing offline. Questo attacco presume che l'aggressore abbia una copia del vostro documento criptato oppure un file di password criptate di un server, e che possa provare una serie di password il più velocemente possibile. Vi sono alcune circostanze in cui tale attacco non ha senso. Le tessere Bancomat, per esempio, sono sicure anche se hanno un codice PIN a quattro cifre, perché non è possibile effettuare il password guessing offline. Ed è più probabile che la polizia ottenga un mandato per il vostro account Hotmail invece di prendersi il disturbo di craccare la password della vostra email. Il sistema key-escrow del vostro programma di crittografia è quasi certamente più vulnerabile della vostra password, così come è vulnerabile qualsiasi "domanda segreta" che avete impostato nel caso vi dimentichiate della password.

Coloro che effettuano il password-guessing offline sono diventati sia più veloci che più intelligenti. AccessData vende un prodotto chiamato Password Recovery Toolkit, o PRTK. A seconda del software che sta attaccando, PRTK può arrivare a provare centinaia di migliaia di password al secondo, e dà la precedenza a password più comuni che non a quelle più oscure.

Quindi la sicurezza delle vostre password dipende da due cose: da qualsiasi dettaglio del software che possa rallentare il password guessing, e da quale ordine, programmi come PRTK, indovino le varie password.

Alcuni software includono routine deliberatamente progettate per rallentare il password guessing. Un buon software crittografico non utilizza la vostra password come chiave crittografica; esiste un processo che converte la password nella chiave crittografica. E il software può rendere tale processo lento quanto vuole.

I risultati sono evidenti. Microsoft Office, per esempio, possiede una conversione password-chiave molto semplice, quindi PRTK può provare 350.000 password di Microsoft Word al secondo su un PC Pentium 4 a 3 GHz, che rappresenta un hardware sufficientemente attuale. WinZip era anche peggio: più di un milione di tentativi al secondo con la versione 7.0. Ma con la versione 9.0, la funzione ramp-up del criptosistema è stata decisamente aumentata: ora PRTK può provare soltanto 900 password al secondo. Anche PGP rende le cose deliberatamente difficili per programmi come PRTK, permettendo anch'esso circa 900 tentativi al secondo.

Nell'attaccare programmi con ramp-up volontariamente lenti, è importante che ogni tentativo conti qualcosa. Un semplice attacco esaustivo a una stringa di sei caratteri minuscoli, da "aaaaaa" a "zzzzzz" contiene più di 308 milioni di combinazioni. Ed è generalmente improduttivo, perché il programma impiega la maggior parte del tempo a provare password improbabili come "pqzrwj".

Secondo Eric Thompson di AccessData, una password tipica è costituita da una radice e da un'appendice. Una radice non è necessariamente rappresentata da una parola del dizionario, ma è comunque qualcosa di pronunciabile. Un'appendice può essere un suffisso (90% dei casi) o un prefisso (10% dei casi).

Perciò il primo attacco che PRTK effettua è provare un dizionario di

circa 1000 password comuni, quali "letmein", "password", "123456" e così via. Poi le riprova combinandole con circa 100 suffissi comuni: "1", "4u", "69", "abc", "!", ecc. Che ci crediate o no, con queste 100.000 combinazioni PRTK già recupera il 24% di tutte le password.

Poi PRTK affronta tutta una serie di dizionari radicali e di appendice sempre più complessi. I dizionari radicali comprendono:

- * Dizionario di parole comuni: 5.000 voci
- * Dizionario di nomi: 10.000 voci
- * Dizionario globale: 100.000 voci
- * Dizionario di pattern fonetici: 1/10.000 di una ricerca esaustiva del carattere

Il dizionario di pattern fonetici è interessante. Non è un vero e proprio dizionario, ma una routine basata sulla catena di Markov che genera stringhe di caratteri pronunciabili in lingua inglese di una lunghezza data. Per esempio, PRTK può generare e provare un dizionario di stringhe di sei caratteri molto pronunciabili, o stringhe di sette caratteri appena pronunciabili. Stanno sviluppando routine di generazione anche per altre lingue.

PRTK effettua anche una ricerca esaustiva di stringhe di quattro caratteri. Passa in rassegna i dizionari con parole minuscole (le più comuni in assoluto), con l'iniziale maiuscola (le seconde più comuni), tutte maiuscole e con la finale maiuscola. Poi passa in rassegna i dizionari con le sostituzioni più comuni: "\$" per "s", "@ per "a", "1" per "l" e così via. Viene incluso anche il cosiddetto "leet speak", che per esempio sostituisce la "e" con "3".

I dizionari di appendice comprendono:

- * Tutte le combinazioni di due caratteri
- * Tutte le date dal 1900 al 2006
- * Tutte le combinazioni di tre caratteri
- * Tutti i singoli simboli
- * Tutti i caratteri singoli + simboli singoli
- * Tutte le combinazioni di due simboli

La "salsa segreta" di AccessData è l'ordine con cui vengono esaminate le varie combinazioni dei dizionari radicali e di appendice. Le ricerche dell'azienda indicano che lo "sweet spot" delle password è rappresentato da una radice di 7-9 caratteri più un'appendice comune, e che è più probabile che un utente scelga una radice difficile da indovinare piuttosto che un'appendice non comune.

Normalmente, PRTK si esegue su una rete di computer. Il password guessing è un compito banalmente distribuibile, e può eseguirsi in background con facilità. Una grande organizzazione come i Servizi Segreti può benissimo installare centinaia di computer per scoprire una password. Una compagnia chiamata Tableau sta costruendo un add-on hardware FPGA specializzato per aumentare la velocità di PRTK con programmi lenti come PGP e WinZip, per un aumento delle prestazioni dell'ordine dei 150-300 tentativi.

Qual è l'efficacia di tutto questo? Eric Thompson stima che, avendo a disposizione un intervallo di tempo compreso fra i 15 e i 30 giorni, il suo software può craccare il 55-65% di tutte le password (ciò dipende in

grande misura dall'applicazione, ovviamente). Sono risultati molto buoni, ma non eccezionali.

Ma questo senza contare i dati biografici. Appena può, AccessData raccoglie qualunque informazione personale possibile sul soggetto prima di cominciare. Se può vedere altre password, può formulare dei tentativi sul tipo di password utilizzate dal soggetto. Quanto grande è la radice impiegata? Che genere di radice è? Il soggetto mette appendici all'inizio o alla fine di parola? Fa uso di sostituzioni? I codici postali sono appendici comuni, per cui vengono aggiunte al file. Stesso dicasi per indirizzi, nomi della rubrica indirizzi, altre password e qualsiasi altro tipo di informazione personale. Questi dati aumentano di un poco il livello di successo di PRTK, ma soprattutto riducono il tempo impiegato da settimane a giorni, persino a ore.

Pertanto, se volete che la vostra password sia difficile da indovinare, dovrete scegliere qualcosa che non figura in nessuno degli elenchi radicali e di appendice. Dovreste mescolare le minuscole e le maiuscole nella parte centrale della radice. Dovreste aggiungere numeri e simboli nel centro della radice, e non come sostituzioni comuni. Oppure inserire l'appendice nel mezzo della radice. Oppure usare due radici unite al centro da un'appendice.

È difficile che venga indovinato anche un elemento che non sta in cima agli elenchi dei dizionari di PRTK, come il dizionario di pattern fonetici di sette caratteri, unito a un'appendice non comune. Altrettanto difficile è una password composta dalle prime lettere di una frase, specialmente se si aggiungono numeri e simboli al miscuglio. E, certamente, queste password saranno difficili da ricordare: per questo dovrete utilizzare un programma come Password Safe (gratuito e open source) per conservarle. (PRTK può testare solo 900 password al secondo di quelle contenute in Password Safe 3.0).

In ogni caso, nulla di tutto questo potrebbe avere importanza, dato che AccessData vende anche un altro programma, Forensic Toolkit, che, fra l'altro, esamina un disco rigido alla ricerca di qualsiasi stringa stampabile. Cerca all'interno dei documenti, nel Registro, nelle email, nei file di swap, nello spazio eliminato del disco... ovunque. Crea un dizionario basato sui risultati della ricerca, e lo passa a PRTK.

E PRTK decodifica più del 50% delle password grazie a questo dizionario soltanto.

Il problema è che la gestione della memoria del sistema operativo Windows lascia dati dappertutto durante il corso normale delle operazioni. Voi scrivete la vostra password in un programma, ed essa viene conservata in qualche parte della memoria. Windows passa la pagina dalla memoria al disco (swap), e diviene la coda di qualche file. Viene quindi spostata in qualche zona remota del vostro disco rigido, e lì rimane indefinitamente. Sotto questo punto di vista, Linux e Mac OS non sono migliori.

Tengo a precisare che niente di tutto questo ha a che vedere con l'algoritmo crittografico o con la lunghezza della chiave. Un algoritmo debole da 40 bit non facilita la vita a questo attacco, e un algoritmo forte a 256 bit non la rende più difficile. Questi attacchi simulano il processo di inserimento della password da parte dell'utente, per cui la grandezza della chiave risultante non è mai un problema.

Per anni ho sostenuto che il sistema più semplice per forzare un prodotto crittografico non è quasi mai quello di rompere l'algoritmo, e che quasi invariabilmente esiste un errore di programmazione che permette di aggirare la matematica e di forzare il prodotto. Qui avviene una cosa assai simile. Il metodo più semplice per indovinare una password non è affatto quello di "indovinarla", ma di sfruttare le insicurezze che appartengono al sistema operativo sottostante.

L'analisi di 34.000 password di MySpace:

<http://www.wired.com/news/columns/0,72300-0.html>

Scegliere le password:

<http://psychology.wichita.edu/surl/usabilitynews/81/Passwords.htm>

<http://www.microsoft.com/windows/IE/community/columns/passwords.msp>

<http://www.brunching.com/passwordguide.html>

AccessData:

<http://www.accessdata.com>

Password Safe:

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

Questo articolo è originariamente apparso su Wired.com.

<http://www.wired.com/news/columns/1,72458-0.html>

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

Commenti dei lettori

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

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

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

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.