

CRYPTO-GRAM
15 luglio 2005

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

Edizione italiana curata da Communication Valley SpA

E-mail: schneier@counterpane.com

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

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

Crypto-Gram in versione originale è anche consultabile in formato RSS:

<<http://www.schneier.com/crypto-gram-rss.xml>>

Gli stessi articoli della newsletter sono disponibili sul blog di Bruce Schneier:

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

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

In questo numero:

L'attacco terroristico a Londra
L'antiterrorismo: una mancanza di immaginazione
CardSystems espone le identità di 40 milioni di persone
Notare l'abuso di dati personali
Un call center indiano vende informazioni sensibili
Le ristampe di Crypto-Gram
Scrivete la vostra password
L'adattabilità dei rivoltosi iracheni
News
Furto organizzato nei retail
Il Canile: Privacy.li
Crittoanalisi di SHA-1
Skin di sicurezza
Le News di Counterpane
Verificare l'efficacia delle misure di sicurezza
L'elusione delle multe per eccesso di velocità
Ridefinire lo spyware
Parlare agli sconosciuti
Commenti dei lettori

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

L'attacco terroristico a Londra

Ero in vacanza la scorsa settimana e non ho avuto ancora molto tempo per leggere o scrivere qualcosa a riguardo dell'attacco dinamitardo a Londra. Per il momento vorrei semplicemente esprimere la mia solidarietà e le mie condoglianze a chi è stato direttamente colpito, e a tutte le brave persone a Londra, in Inghilterra, in Europa e nel mondo. Prendere di mira gli innocenti può essere una tattica molto efficace, ma è una cosa altrettanto vigliacca e spregevole.

Vorrei anche invitare tutti a non farsi prendere troppo dai dettagli della tattica dei terroristi. Dobbiamo resistere alla tentazione di reagire ai particolari di questa specifica trama terroristica: occorre rimanere concentrati sugli obiettivi dei terroristi. Spendere miliardi per proteggere treni e autobus a scapito di altre contromisure antiterrorismo non ha alcun senso. I terroristi hanno come scopo il provocare terrore, e a loro non importa bombardare treni, metropolitane, autobus, centri commerciali, cinema, scuole, supermercati, ristoranti, discoteche o qualsiasi altro luogo atto a contenere cento e più persone. Semplicemente, i bersagli da difendere sono troppi, e dobbiamo pensare a qualcosa di più intelligente che non il proteggere gli specifici bersagli dell'ultimo attentato terroristico avvenuto due settimane fa.

Misure antiterrorismo più brillanti si concentrano sui terroristi e come vengono finanziati - - fermando i loro piani a prescindere dai bersagli del momento -- nonché sulla risposta in caso di emergenza, per ridurre i danni da essi provocati.

Avrò da dire molto di più il mese prossimo. Ancora, intendo esprimere tutta la mia solidarietà alle vittime e ai feriti, alle loro famiglie e ai loro amici, e a tutti coloro nel mondo che vengono indirettamente colpiti da questi episodi, che i media continuano ripetutamente a presentare.

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

L'antiterrorismo: una mancanza di immaginazione

Il rapporto della Commissione per l'11 settembre ha parlato di una "mancanza di immaginazione" prima degli attacchi dell'11 settembre: "Una delle mancanze più gravi è stata a livello di immaginazione. Non crediamo che i leader avessero compreso la gravità della minaccia. Il pericolo terroristico rappresentato da Bin Laden e dal Al Qaeda non era uno degli argomenti di maggior importanza nel dibattito politico a livello pubblico, di mass media, o governativo. Anzi, se n'è parlato a malapena durante la campagna presidenziale del 2000".

Più in generale, questa espressione è stata usata per descrivere la risposta del Governo degli Stati Uniti alla minaccia terroristica. Si spende moltissimo denaro per difenderci da quello che i terroristi hanno fatto nell'attacco precedente, o da particolari minacce che immaginiamo, ma ignoriamo la minaccia nella sua totalità o le cause che stanno alla radice del terrorismo.

Dopo l'attacco a Londra, ci stiamo ricascando. Stavo per scrivere un lungo intervento a questo riguardo, ma Richard Forno ha già scritto un ottimo articolo.

L'articolo di Forno:

<<http://www.infowarrior.org/articles/2005-01.html>>

Il Rapporto della Commissione 9/11:

<<http://www.washingtonpost.com/wp-srv/nation/911report/documents/911ReportExec.pdf>> oppure <<http://tinyurl.com/3vojj>>
<http://en.wikipedia.org/wiki/Failure_of_imagination>

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

CardSystems espone le identità di 40 milioni di persone

Le informazioni personali di più di 40 milioni di persone sono state vittima di hacking. L'hacking è avvenuto alla CardSystems Solutions, una società che processa transazioni di carte di credito. I dettagli dell'accaduto non sono ancora chiari. Il New York Times scrive che "i dati di circa 200.000 conti di MasterCard, Visa e altre compagnie di carte di credito sono stati sottratti a seguito della violazione", anche se la vulnerabilità era estesa a 40 milioni di individui. Il furto è il prodotto di un hacking malevolo e premeditato, credo il primo in questa serie di recenti abusi di dati sensibili. Negli altri casi il tutto è stato accidentale (nastri di backup che se ne vanno a spasso, per esempio) o si è trattato di attacchi di ingegneria sociale. Qui invece qualcuno era a caccia di questi dati, e ciò significa una maggiore probabilità che ci scappi la frode, a differenza del caso dei nastri di backup andati dispersi.

CardSystems sostiene di aver trovato il problema. Di contro, anche MasterCard ha dichiarato di averlo trovato. Il New York Times sostiene MasterCard. La colpa potrebbe essere del software di Microsoft. E in un bizzarro colpo di scena, CardSystems ha ammesso che non era nemmeno tenuta a mantenere quei dati in prima istanza.

Dal New York Times: "John M. Perry, direttore generale di CardSystems Solutions [...] ha detto che i dati si trovavano in un file archiviato 'a scopo di effettuare ricerche' per determinare perché alcune transazioni erano state registrate come non autorizzate o incomplete".

Sì, certo. Ricerca = marketing, ci scommetto.

Questo è esattamente il genere di guai che Visa e MasterCard stanno facendo di tutto per prevenire. Hanno imposto i loro propri requisiti di sicurezza a tutte le società e aziende che gestiscono a vari livelli i dati delle carte di credito. Il programma di sicurezza di Visa si chiama CISP, Cardholder Information Security Program. Quello di MasterCard prende il nome di SDP, Site Data Protection. I programmi sono stati combinati in uno standard di sicurezza congiunto chiamato PCI, che coinvolge anche Discover, American Express, JCB e Diners Club in certa misura.

I requisiti di PCI riguardano la sicurezza di rete, la gestione delle password, la cifratura

dei dati archiviati, il controllo degli accessi, il monitoraggio, le verifiche, le linee di condotta, ecc. E le compagnie di carte di credito sostengono questi requisiti a suon di pesanti sanzioni: multe fino a 100.000 dollari, aumento delle commissioni per le transazioni, e risoluzione del conto. Per un commerciante che svolge gran parte della propria attività tramite circuiti di carte di credito, questo è un grosso incentivo a conformarsi.

Non si tratta di leggi, ma di requisiti di un contratto d'affari. Non vengono imposti dal governo: sono le compagnie di carte di credito che li richiedono per proteggere i propri brand.

Ogni compagnia di carte di credito è spaventata dalla possibilità che la gente faccia un uso sempre meno continuato delle carte di credito. Le compagnie di carte di credito sono preoccupate dal fatto che tutta questa rilevanza data dalla stampa al furto di dati sensibili, al furto di identità e ad altri tipi di frode ai danni delle carte di credito, allontanerà gli acquirenti da Internet. Sono preoccupate dall'idea che il pubblico possa farsi del loro brand. E non vogliono che qualche stupida società rovini la loro reputazione esponendo più di 40 milioni di possessori di carte di credito al rischio di frode (o dando ai giornalisti l'opportunità di scrivere titoloni come "CardSystems Solutions mette in mano agli hacker 40 milioni di carte di credito").

Essendo indipendenti da leggi o regolamentazioni governative, le compagnie di carte di credito stanno obbligando le aziende che processano dati di carte di credito ad aumentare la loro sicurezza. Le aziende devono conformarsi al programma PCI oppure affronteranno gravi conseguenze.

CardSystem era in piena conformità? Avrebbe dovuto conformarsi al programma CISP di Visa entro il 30 settembre 2004, e di certo si trovava nel livello di servizio più alto (la conformità a PCI non era obbligatoria fino al 30 giugno 2005, circa due settimane dopo l'annuncio della violazione). La realtà dei fatti è piuttosto oscura.

Ancora dal New York Times:

"Dopo la divulgazione della falla di sicurezza di CardSystems, sono stati forniti diversi resoconti in merito alla conformità dell'azienda agli standard imposti dall'associazione delle compagnie di carte di credito.

"Jessica Antle, una portavoce di MasterCard, ha dichiarato che CardSystems non ha mai dimostrato conformità agli standard di MasterCard. 'Erano in aperta violazione delle nostre regole', ha detto.

"Non è chiaro se o quando MasterCard sia intervenuta in passato con questa azienda per assicurarne la conformità, ma MasterCard ha dichiarato venerdì scorso di aver dato ora a CardSystem 'un periodo molto ristretto' per farlo.

"Interpellata sulla conformità agli standard di Visa, una portavoce di Visa, Rosetta Jones, ha dichiarato: 'Questa azienda in particolare non stava rispondendo ai requisiti di sicurezza richiesti da Visa quando abbiamo scoperto una potenziale compromissione di dati'.

“Precedentemente Perry, il direttore di CardSystems, ha dichiarato che la sua società fu verificata nel dicembre 2003 da una non meglio specificata agenzia indipendente e che ha ricevuto un sigillo di approvazione dalle associazioni di pagamento Visa nel giugno 2004”.

Tutto questo mette in luce alcune limitazioni di un qualsiasi sistema di certificazione. Primo, le società possono avvantaggiarsi di politiche interpersonali e interaziendali per ottenere per se stesse trattamenti speciali per quanto concerne le linee di condotta. E in secondo luogo, tutte le verifiche si appoggiano in larga misura sull'autovalutazione e su un livello di apertura deciso autonomamente. Se un'azienda vuole mentire a un auditor, è improbabile che venga scoperta.

A meno che non venga palesemente scoperta grazie a incidenti come quello accaduto.

Autodenunciarsi funziona soltanto se la pena è largamente superiore al reato. Il motivo per cui la gente nei moduli doganali dichiara accuratamente quel che porta all'interno del paese, per esempio, è perché le sanzioni che colpiscono chi mente sono molto maggiori e più costose del pagare il dovuto.

Se l'industria delle carte di credito vuole che i propri requisiti PCI siano presi sul serio, occorre che faccia di CardSystems un esempio per tutti. È necessario revocare ogni licenza di gestione carte di credito concessa a CardSystems, al massimo grado possibile stabilito da qualsiasi contratto abbiano precedentemente stipulato. Solo facendo di CardSystems la dimostrazione di quanto accade se qualcuno non rispetta le regole, tutti gli altri capiranno che è meglio conformarsi.

(CardSystems dovrebbe anche essere perseguita penalmente, ma è difficile che succeda nell'attuale sistema politico, molto "amichevole" verso le aziende).

Ho grandi speranze per il programma PCI. Preferisco soluzioni di sicurezza che prevedano un contratto fra aziende che un intervento governativo. Spesso il secondo è necessario, ma il primo è molto più efficace. Ora è l'occasione per PCI di dimostrare la propria efficacia.

Gli articoli che parlano della notizia:

<<http://news.bbc.co.uk/2/hi/americas/4107236.stm>>

<<http://www.computerworld.com/securitytopics/security/story/0,10801,102631,00.html>

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

<<http://www.merit.edu/mail.archives/netsec/msg00625.html>>

<<http://businessweek-cnet.com/CardSystems+Well+meet+security+goals>

+soon/2100-1029_3-5780265.html> oppure <<http://tinyurl.com/a5wcy>>

<<http://techrepublic.com.com/5254-6257-0.html?forumID=99&threadID=17409>

5&messageID=1794064&id=4137111>

oppure <<http://tinyurl.com/ck79c>>

<[http://news.softpedia.com/news/Microsoft-Software-to-Blame-for-the-CardSystems-](http://news.softpedia.com/news/Microsoft-Software-to-Blame-for-the-CardSystems-Data-Security-Breach-3440.shtml)

[Data-Security-Breach-3440.shtml](http://news.softpedia.com/news/Microsoft-Software-to-Blame-for-the-CardSystems-Data-Security-Breach-3440.shtml)> oppure <<http://tinyurl.com/76gla>>

<[http://news.softpedia.com/news/CardSystems-Solutions-hands-over-40M-credit-cards-](http://news.softpedia.com/news/CardSystems-Solutions-hands-over-40M-credit-cards-to-hackers-3367.shtml)

[to-hackers-3367.shtml](http://news.softpedia.com/news/CardSystems-Solutions-hands-over-40M-credit-cards-to-hackers-3367.shtml)> oppure <<http://tinyurl.com/8dxo7>>

Comunicati stampa di CardSystems e MasterCard:

<<http://www.cardsystems.com/news.html>>
<<http://www.mastercardinternational.com/cgi-bin/newsroom.cgi?id=1038>>

CISP, SDP, e PCI:

<http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html?it=12|/business/accepting_visa/ops_risk_management/cisp_merchants.html|CardholderInformationSecurityProgram> oppure <<http://tinyurl.com/96544>>
<<https://sdp.mastercardintl.com/>>
<http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_PCI_Data_Security_Standard.pdf> oppure <<http://tinyurl.com/4ph6h>>
<http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_service_providers.html> oppure <<http://tinyurl.com/bzzsh>>

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

Notare l'abuso di dati personali

Ognuno sembra guardare ai propri database cercando eventuali fughe di informazioni personali. Ecco un articolo:

"Crediti fiscali, documenti d'ipoteca, atti notarili e altri documenti legati all'ambito immobiliare sono disponibili pubblicamente in database online gestiti da uffici di registrazione di atti legali in tutto lo stato. In database liberamente accessibili di tutte le contee del Massachusetts eccetto tre, il Globe ha trovato documenti contenenti i nomi e i numeri di previdenza sociale dei residenti del Massachusetts...

"Anche se gli uffici di registrazione hanno dichiarato di non conoscere casi in cui dei criminali si siano serviti di informazioni contenute nei database, i dati presenti nei documenti sarebbero più che sufficienti per commettere un furto di identità e aprire nuove linee di credito..."

Ma questo non è appunto parte del problema? È facile dire "non abbiamo visto casi di frode che hanno sfruttato le nostre informazioni", perché raramente esiste un sistema per stabilire da dove derivano le informazioni. La recente epidemia di fughe di dati deriva da persone che hanno notato queste fughe, e non dagli effetti causati dalle fughe stesse. Quindi ognuno ritiene che le proprie modalità di gestione dei dati siano buone, perché non vi sono mai stati abusi documentati che siano partiti da fughe di quei dati, e non fa altro che ingannarsi.

<http://www.boston.com/business/technology/articles/2005/06/23/states_online_record_s_pose_risk/> oppure <<http://tinyurl.com/axgr7>>

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

Un call center indiano vende informazioni sensibili

La Coca-Cola e la NSA:

<<http://www.schneier.com/crypto-gram-0407.html#8>>

<<http://www.cryptogram.it/cryptogramPdf/Luglio2004.pdf>> (versione italiana)

Come reagire:

<<http://www.schneier.com/crypto-gram-0307.html#1>>

<<http://www.cryptogram.it/luglio03.htm#a1>> (versione italiana)

I falsi allarmi:

<<http://www.schneier.com/crypto-gram-0307.html#8>>

<<http://www.cryptogram.it/luglio03.htm#a8>> (versione italiana)

Sistemi di controllo incorporati e Sicurezza

<<http://www.schneier.com/crypto-gram-0207.html#1>>

<<http://www.cryptogram.it/luglio02.htm#a1>> (versione italiana)

La nuova generazione dell'hacking telefonico:

<<http://www.schneier.com/crypto-gram-0107.html#1>>

Il monitoraggio innanzitutto:

<<http://www.schneier.com/crypto-gram-0107.html#5>>

L'esposizione totale e la CIA:

<<http://www.schneier.com/crypto-gram-0007.html#1>>

Unicode e i rischi legati alla sicurezza:

<<http://www.schneier.com/crypto-gram-0007.html#9>>

Il futuro del "Crypto-Hacking":

<<http://www.schneier.com/crypto-gram-9907.html#hacking>>

I pasticci e le approssimazioni di SSL:

<<http://www.schneier.com/crypto-gram-9907.html#doghouse>>

La declassificazione di Skipjack:

<<http://www.schneier.com/crypto-gram-9807.html#skip>>

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

Scrivete la vostra password

Lo scorso mese, Jesper Johansson di Microsoft ha fatto notizia invitando le persone ad annotarsi le proprie password. È un ottimo consiglio, che ho ripetuto per anni.

Semplicemente, la gente non è più in grado di ricordare password sufficientemente valide per contrastare i dictionary attack, e si ottiene una sicurezza molto maggiore se si sceglie una password troppo complessa da ricordare e la si scrive da qualche parte. Siamo tutti dei maestri quando si tratta di mettere al sicuro piccoli pezzi di carta. Io consiglio di

scrivere le vostre password più importanti su un pezzetto di carta e poi di tenerlo al sicuro insieme ad altri pezzetti di carta importanti, cioè nel vostro portafogli. Per una maggiore sicurezza certi riferimenti possono essere oscuri o generici: scrivete "banca" invece dell'URL completo della vostra banca, scambiate qualche carattere, non includete il vostro nome utente. Questo vi darà un po' più di tempo se smarrite il portafogli e dovete cambiare tutte le password. Ma anche se non state a fare tutto questo, annotarvi la vostra password impossibile-da-memorizzare è sempre più sicuro che semplificare la password per poterla ricordare.

<http://news.com.com/Microsoft+security+guru+Jot+down+your+passwords/2100-7355_3-5716590.html> oppure <<http://tinyurl.com/8tuz3>>

Oppure potete usare PasswordSafe:
<<http://www.schneier.com/passsafe.html>>

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

L'adattabilità dei rivoltosi iracheni

Questo articolo di Newsweek sui rivoltosi in Iraq comprende un paragrafo molto interessante su come essi si adattino alle difese militari americane.

"Gli esperti di controinsorgenza sono allarmati dalla velocità con cui le tattiche del fronte opposto riescono ad evolversi. Un caso particolarmente preoccupante è il braccio di ferro continuato in ambito di ordigni esplosivi improvvisati. I primi ordigni esplosivi improvvisati venivano detonati da cavi e batterie; i rivoltosi aspettavano al lato della strada e facevano brillare gli ordigni primitivi al passaggio di veicoli americani. In seguito le truppe USA sono diventate esperte nell'individuare e uccidere chi faceva brillare le bombe. Questo ha portato i rivoltosi a sostituire i cavi con segnali radio. Il Pentagono, a velocità frenetica e spendendo un patrimonio, ha equipaggiato l'esercito con dei jammer per bloccare quei segnali, riuscendo nell'intento questa primavera. I rivoltosi hanno reagito prontamente inviando un segnale radio continuo all'ordigno esplosivo improvvisato; quando il segnale viene fermato o deviato, la bomba esplode. La soluzione? Intercettare il segnale e fare in modo che continui. Problema: il segnale è criptato. Ora gli americani sono alle prese con il compito di decodificare la crittografia al volo ed imitarla -- finora senza successo. Comunque i morti causati da questi ordigni esplosivi improvvisati sono diminuiti, dato che le truppe USA possono interrompere il segnale e innescare l'ordigno prima che passi un convoglio. Questa è la buona notizia. La cattiva notizia è che il nuovo sistema di detonazione la dice lunga sulle capacità tecniche dei rivoltosi.

La CIA è preoccupata dal fatto che l'Iraq sta diventando un vivaio di terroristi ancor peggiore e più efficace di quanto lo sia mai stato l'Afghanistan, poiché essi si fanno subito un'esperienza sul campo con tecniche di guerriglia urbana in pieno stile terroristico.

<<http://www.msnbc.msn.com/id/8272786/site/newsweek/>>

** **

News

La sicurezza aerea sta diventando surreale: "...una norma della FAA che richiede ai soldati -- tutti quanti armati con un arsenale di fucili d'assalto, doppiette e pistole -- di consegnare coltellini tascabili, forbici per la peluria nasale, e accendini".

<http://www.ajc.com/news/content/custom/blogs/guard/entries/2005/05/19/drop_those_nose_hair_clippers_soldier.html> oppure <<http://tinyurl.com/7z8my>>

"Una stupida coerenza è l'ossessione di piccole menti" -- Ralph Waldo Emerson

Questo documento è del 2003, ma non lo avevo mai visto prima: "Analysis of the MediaMax CD3 Copy-Prevention System" [Analisi del sistema anticopia MediaMax CD3].

<<http://www.cs.princeton.edu/~jhalderm/cd3/>>

La storia secondo cui Dell venderebbe computer con keyboard logger incorporati è una burla.

<<http://c0x2.de/lol/lol.html>>

<<http://www.snopes.com/computer/internet/dellbug.asp>>

Lo Underhanded C Contest è, per quanto ne so, l'unica competizione di programmazione legata alla sicurezza. L'obiettivo è scrivere codice C chiaro e leggibile, ma con un comportamento malevolo nascosto; in altre parole, nascondere materiale malevolo in un codice che passi l'ispezione visiva del sorgente da parte di altri programmatori.

<<http://www.brainhz.com/underhanded/>>

Ecco un'applicazione interessante dell'identificazione mediante DNA. Si tratta di uno spray che viene automaticamente rilasciato se viene aperta una porta, spruzzando una polverina addosso al ladro. Poi, invece di cercare il vostro DNA sulla scena del crimine, le forze dell'ordine cercano il DNA della scena del crimine su di voi.

<http://news.bbc.co.uk/1/hi/wales/north_east/4566991.stm>

Dell Computer richiede obbligatoriamente l'uso che farete con il vostro nuovo computer, a causa del PATRIOT Act.

<<http://www.skippy.net/blog/2005/06/09/security-through-stupidity/>>

Seagate ha introdotto un nuovo hard disk che permette la crittografia dell'intero disco.

<<http://www.computerworld.com/securitytopics/security/story/0,10801,102649,00.html>

> oppure <<http://tinyurl.com/bw872>>

<<http://www.eweek.com/article2/0,1759,1825740,00.asp>>

Qui c'è il comunicato stampa, e l'altro link punta alle specifiche del prodotto. Ignorate la scritta "TDEA 192", è un refuso: il prodotto utilizza triple-DES, e la nuova versione del disco userà AES.

<<http://www.seagate.com/cda/newsinfo/newsroom/releases/article/0,,2732,00.html>>

oppure <<http://tinyurl.com/9wjo8>>

<<http://www.seagate.com/content/docs/pdf/marketing/PO-Momentum-FDE.pdf>>

Un'intervista interessante a Marcus Ranum:

<<http://www.securityfocus.com/columnists/334>>

Il Dipartimento di Giustizia degli Stati Uniti vuole che il vostro ISP vi spii:
<http://news.com.com/Your+ISP+as+Net+watchdog/2100-1028_3-5748649.html>
oppure <<http://tinyurl.com/7s49k>>

Ottimo editoriale di Wired sul furto d'identità. Comprende precisi consigli rivolti al Congresso.

<<http://wired.com/news/privacy/0,1848,67845,00.html>>

Non lo metterò nel Canile, perché mi sembra della buona tecnologia bistrattata da stupidi addetti alle Pubbliche Relazioni: "Il network che è stato appena sviluppato, hanno detto i ricercatori, è compatibile con i protocolli Internet già esistenti, il che significa che le attuali applicazioni Internet potranno usare tecniche di trasmissione standard e anche crittografia ad alto livello fino a 256 bit e oltre, che è al momento il doppio del valore ritenuto essenziale per avere delle transazioni online sicure".

<http://www.wirelessnewsfactor.com/story.xhtml?story_id=11300002GZES>

Un'analisi di sicurezza della macchina per il voto Opti-Scan di Diebold (scheda cartacea).

<<http://www.bbvforums.org/cgi-bin/forums/board-auth.cgi?file=/1954/5921.html>>

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

Una divertente animazione Flash che mostra un'opinione "musicale" sulla carta di identità nazionale britannica proposta da Clarke.

<<http://ecltech.co.uk/clarkeidcards.php>>

Storia interessante sul mercato nero dei dati a Mosca:

<<http://attrition.org/errata/dataloss/russia02.html>>

Questa tecnologia di scansione del corpo -- detta Millimeter-Wave Detection -- è meno invasiva della tecnologia raggi X a retrodiffusione.

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

Lo Hymn Project esiste per aggirare lo schema di protezione degli mp4 di iTunes, in modo che possiate ascoltare la musica che avete comprato su qualsiasi computer vogliate. Inizialmente, il software recuperava la vostra password iTunes (la chiave, sostanzialmente) dall'hard disk. In risposta, Apple ha offuscato il formato e nessuno è ancora riuscito a trovare un sistema per recuperare le chiavi in modo pulito. Per aggirare tutto questo, Hymn Project ha creato un programma chiamato FairKeys che finge di essere iTunes e contatta il server. Dato che il client iTunes può ancora ottenere la vostra password, il trucco funziona. Maggiore sicurezza tramite scomodità, e un'ennesima dimostrazione dell'infinito braccio di ferro tra aggressore e difensore.

<<http://www.hymn-project.org/>>

<http://www.hymn-project.org/jhymndoc/jhymn_faq.php#fairkeys>

Sono stato ottimamente citato in questo articolo del New York Times sul furto di identità:

<<http://www.nytimes.com/2005/07/09/business/09nocera.html>>

Un articolo interessante sulla particolare forma d'arte della fotografia di strada (street photography). Un paragrafo inquietante: "Più gravose sono le restrizioni a seguito dell'11 settembre, che hanno posto dei limiti alla fotografia in luoghi pubblici. Tucker ha ricevuto

email da vari professionisti trattenuti dalle autorità per aver fotografato ponti e treni sopraelevati. 'Vi sono luoghi in cui fotografare la gente per strada potrebbe diventare illegale', osserva Westerbeck". Che tristezza.

<<http://csmonitor.com/2005/0708/p12s01-alar.html>>

La polizia ha arrestato un uomo per aver utilizzato la connessione a Internet tramite rete wireless di un'altra persona senza chiedere il permesso. A quanto mi è dato di capire, non c'è stata nessun'altra attività criminale. Il tizio che ha usato la rete wireless altrui non stava facendo nulla di male, solo navigando in Internet. Credo si tratti del primo caso penale che riguardi questa pratica piuttosto comune.

<<http://www.cnn.com/2005/LAW/07/07/wi.fi.theft.ap/index.html>>

Un libro pubblicato di recente afferma che Himmler è stato assassinato dal British Special Operations Executive (il servizio britannico per le operazioni speciali) e non si è suicidato dopo essere stato catturato dagli Alleati. Il libro si è basato su documenti trovati -- apparentemente in buona fede -- nell'Archivio di Stato del Regno Unito; documenti che ora pare siano stati falsificati e inseriti. Sembra che gli sforzi della sicurezza dell'Archivio di Stato siano mirati ad evitare che i documenti vengano sottratti. Ma gli effetti di aggiungere documenti falsificati potrebbero essere ancora peggiori.

<<http://news.telegraph.co.uk/news/main.jhtml?xml=/news/2005/07/02/nhimmler02.xml>

> oppure <<http://tinyurl.com/cyko3>>

<<http://opinion.telegraph.co.uk/opinion/main.jhtml?xml=/opinion/2005/07/02/di0203.xml>

> oppure <<http://tinyurl.com/8vqlg>>

Ho già scritto della stupidità del preoccuparsi per i telefoni cellulari sugli aerei. Ora il Dipartimento per la Sicurezza Nazionale è preoccupato dell'Internet a banda larga, e vuole poter essere in grado di iniziare a intercettare l'uso di internet di ogni passeggero entro 10 minuti dall'ottenimento dell'autorizzazione da parte di un giudice. I terroristi non usano mai SSH, dopotutto. (Suppongo che questa è la prossima cosa che il Dipartimento per la Sicurezza Nazionale cercherà di vietare).

<<http://wirednews.com/news/technology/0,1282,68147,00.html>>

Il NIST (l'Istituto Nazionale USA per gli Standard e le Tecnologie) ha pubblicato una bozza di un documento dal titolo "Special Publication 800-56, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm

Cryptography" [Pubblicazione Speciale 800-56, Indicazione per gli schemi di impostazione di chiavi pair-wise utilizzando crittografia a logaritmo discreto]. È in cerca di commenti prima che il documento venga completato. Inviare un commento a ebarker@nist.gov entro venerdì 19 agosto, specificando "Comments on SP800-56" come oggetto dell'email.

<http://csrc.nist.gov/CryptoToolkit/kms/SP800-56_7-5-05.pdf>

Syndication RSS sicura:

<<http://www.xml.com/pub/a/2005/07/13/secure-rss.html>>

Stavo per scrivere qualcosa sulla stupidità di installare telecamere in luoghi pubblici come risposta alle minacce terroristiche, ma Scott Henson mi ha preceduto:

<<http://gritsforbreakfast.blogspot.com/2005/07/cameras-wrong-response-to-london.html>> oppure <<http://tinyurl.com/74ang>>

Secondo il Times di Londra: "Fonti di sicurezza hanno confermato che nessuno dei terroristi dinamitardi era presente nei registri MI5, anche se uno aveva collegamenti a un individuo sotto indagine".

<http://www.timesonline.co.uk/article/0,,22989-1692540_1,00.html>

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

Furto organizzato nei retail

Vi sono due diverse minacce che riguardano il taccheggio: il piccolo taccheggio e il furto organizzato nei retail. "Il reato di furto organizzato nei retail è qualcosa di separato e ben distinto dal piccolo taccheggio, in quanto coinvolge circoli di ladri che si spostano rapidamente di comunità in comunità e attraverso gli stati per rubare grandi quantità di prodotti che vengono poi riconfezionati e rivenduti al mercato. Il piccolo taccheggio, per definizione, è limitato a oggetti sottratti per uso o consumo personale".

Il loro elenco dei 50 oggetti più rubati consiste di piccoli e costosi prodotti che hanno vita lunga sugli scaffali: per la maggior parte farmaci a vendita libera (senza ricetta medica).

- #1 Advil compresse 50 ct
- #2 Advil compresse 100 ct
- #3 Aleve capsule 100 ct
- #4 EPT test di gravidanza
- #5 Gillette Sensor 10 ct
- #6 Kodak 200 24 esp.
- #7 Similac con polvere di ferro - scatola
- #8 Similac con polvere di ferro - conf.singola
- #9 Preparation H 12 ct
- #10 Primatene compresse 24 ct

<<http://www.fmi.org/loss/ORT/>>

<http://www.fmi.org/loss/ORT/top50_shoplifted_items.pdf>

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

Il Canile: Privacy.li

Questa azienda presenta sul proprio sito una descrizione che scalda il cuore: "Privacy dal Principato del Liechtenstein, nel cuore delle Alpi, nascosto fra la Svizzera e l'Austria. In tempi di inquietudine e di insicurezza, cacce alle streghe e sospetti, espropriazioni e diminuita credibilità dei leader mondiali, è sempre bello poter avere un luogo a cui affidarsi. Questo è l'umile sforzo di mettere a disposizione dei cittadini del mondo preoccupati per la privacy e le libertà un luogo per incontrarsi, discutere, aiutarsi e nutrire i propri desideri di libertà".

Però non hanno alcuna intenzione di far sapere ai loro clienti nulla che li riguardi: "Profilo

della società -- In effetti non deve essere pubblicato qui :-) Un servizio di privacy come il nostro funziona al meglio se non vengono divulgati troppi dettagli - ci auguriamo che comprendiate e sosteniate questo aspetto. Chi ha creato questa pagina sono degli esperti in materia, e non metteranno a rischio la vostra privacy per nessun motivo”.

Ah, sicuro. E il prodotto “DriveCrypt” che vendono comprende “una crittografia real time a 1344 bit, di potenza militare”.

Chissà perché, il mio cuore non è più così caldo.

<<http://www.privacy.li/>>
<<http://www.privacy.li/drivecrypt.htm>>

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

Crittoanalisi di SHA-1

A febbraio ho scritto di un gruppo di ricercatori cinesi che avevano violato la funzione hash di SHA-1. Quell’intervento si basava su un breve preavviso da parte dei ricercatori. Da quel momento mi hanno scritto in molti, chiedendomi notizie della ricerca e della documentazione, alcuni dubitando della validità della ricerca a causa della mancanza di documentazione.

Lo studio c’è, ne ho vista una copia. I ricercatori lo presenteranno alla Crypto conference ad agosto. Ritengo che non l’abbiano pubblicata perché Crypto richiede che gli studi inviati non siano stati già pubblicati, e i ricercatori hanno frainteso il requisito pensando che lo studio non potesse essere diffuso in alcun modo.

Ora ve n’è una copia sul Web, ed è possibile leggere “Finding Collisions in the Full SHA-1” [Ricerca collisioni nello SHA-1 completo] a cura di Xiaoyun Wang, Yiqun Lisa Yin, e Hongbo Yu.

Lo studio:
<http://cryptome.org/wang_sha1_v2.zip>
<http://www.schneier.com/blog/archives/2005/02/cryptanalysis_o.html>
<<http://theory.csail.mit.edu/~yiqun/shanote.pdf>>

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

Skin di sicurezza

Molto è stato scritto in merito all’insicurezza delle password. Oltre a essere indovinabili, la gente si fa sempre più ingannare offrendo le proprie password a server illegali perché non riesce a distinguere finestre e pagine Web falsificate da quelle regolari.

Recensione di "Beyond Fear":

<<http://www.securitypipeline.com/164902244;jsessionid=NPFSUEUTX5MVEQSNDBGCKH0CJUMEKJVN>> oppure <<http://tinyurl.com/958y5>>

Recensione di "Secrets and Lies":

<<http://www-128.ibm.com/developerworks/rational/library/mar05/reader/higgins.html>> oppure <<http://tinyurl.com/agxbn>>

Lo scorso dicembre ho rilasciato una lunga intervista a una rivista letteraria chiamata Turnrow. L'intervista è stata finalmente pubblicata, ed è ancora migliore di quanto la ricordassi:

<<http://turnrow.ulm.edu/bruceschneierinterview.htm>>

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

Verificare l'efficacia delle misure di sicurezza

In mezzo a tutta la retorica emotiva che si incontra in tema di sicurezza, è bello vedere ogni tanto qualcosa di razionale e ponderato. Un editoriale di opinione del New York Times, a firma Nicholas Kristof, pubblicato agli inizi del mese guarda alla sicurezza come a un compromesso, e traccia una distinzione fra misure di sicurezza che riducono una minaccia e misure di sicurezza che la spostano semplicemente.

Ho scritto di questo in "Beyond Fear": "Un ladro che nota la presenza di un sistema d'allarme andrà molto probabilmente a svaligiare la casa di un altro. Dal punto di vista del comando di polizia locale, ciò non mitiga affatto il rischio. Ma per il padrone di casa il rischio è ottimamente mitigato".

La differenza sta nella prospettiva del difensore.

I problemi con le prospettive sono evidenti nelle difese antiterrorismo, tutte le volte. Sempre da "Beyond Fear": "È importante non perdere di vista il panorama generale focalizzandosi soltanto sul particolare. Le contromisure di sicurezza spesso si concentrano sulla prevenzione di atti terroristici ai danni di bersagli specifici, ma l'ambito delle risorse che devono essere protette comprende tutti i bersagli possibili, e devono essere considerati tutti insieme. Il vero bersaglio di un terrorista è lo stato d'animo, e non gli importa davvero di questo o quel bersaglio fisico. Vogliamo prevenire atti terroristici ovunque, per cui le misure di sicurezza che spostano semplicemente la minaccia hanno un valore quanto mai limitato. Se, per esempio, investiamo moltissimo denaro per difendere centri commerciali, e poi gli attacchi dinamitardi hanno luogo in stadi affollati o nei cinema, non abbiamo ottenuto alcun valore e vantaggio dalle nostre contromisure".

<<http://www.newsobserver.com/print/thursday/opinion/story/2548446p-8952410c.html>> oppure <<http://tinyurl.com/b8hss>>

Sono felice di vedere linee di pensiero come questa apparire nei media, e mi piacerebbe che ciò capitasse più spesso.

** **

L'elusione delle multe per eccesso di velocità

A prescindere da quel che pensate sulla moralità di guidare oltre i limiti di velocità, questo è un campo molto diffuso per quanto concerne la sicurezza... un campo per cui ogni automobilista nutre almeno un po' di interesse.

Il sito Radarbusters è gestito da un ex poliziotto, e trasmette autorevolezza. Mette molta enfasi sull'educazione; installare uno stravagante rilevatore di radar non vi servirà a molto, a meno che non sappiate come utilizzarlo correttamente (e fra parentesi, il tizio vende il rilevatore che consiglia).

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

Ecco un prodotto che pare contrastare la minaccia degli scanner aerei di targhe automobilistiche.

<<http://www.radarbusters.com/products/photo-radar/Overhead-Protector.asp>> oppure

<<http://tinyurl.com/a5292>>

<http://www.schneier.com/blog/archives/2005/04/licenseplate_sc.html>

Questo spray dovrebbe rendere la targa della vostra auto invisibile alle fotocamere. Non ho idea se funzioni.

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

Una nota conclusiva: l'ex poliziotto offre una ricompensa di 5.000 dollari alla prima persona che gli indichi un jammer laser passivo che funzioni davvero.

<<http://www.radarjammer.com/get-5000/index.htm>>

** **

Ridefinire lo spyware

Il problema con lo spyware è che può essere nell'occhio di chi guarda. Vi sono aziende che sminuiscono il problema generale, ma hanno il proprio software che "fa rapporto" a un server centrale.

Questo genere di cose può sfociare in un conflitto di interesse: "Lo spyware è tale solo se non ho alcun interesse aziendale in esso". Ecco l'esempio più recente: "L'applicazione AntiSpyware di Microsoft Windows non segnala più i prodotti di Claria Corp. come minacce per gli utenti PC. A meno di una settimana dalla pubblicazione della notizia di colloqui di acquisizione fra Microsoft e l'azienda californiana distributrice del controverso software pubblicitario Gator, i ricercatori di sicurezza hanno scoperto che Microsoft ha tacitamente disattivato i rilevamenti dei prodotti di Claria".

Se utilizzate AntiSpyware, potete rimediare a questo. Lo spyware di Claria è ora impostato su "Ignore" [Ignora] per default, ma potete ancora modificarlo in "Quarantine"

[Quarantena] o "Remove" [Elimina]. Io consiglio "Remove". Anzi, consiglio di usare un altro prodotto.

<<http://www.eweek.com/article2/0,1895,1834607,00.asp>>

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

Parlare agli sconosciuti

In "Beyond Fear" ho scritto: "A molti bambini viene insegnato di non parlare mai con gli sconosciuti, una precauzione estrema che apporta scarsissimi benefici di sicurezza".

Nelle conversazioni, sono ancora più diretto. Credo che "non parlare mai con gli sconosciuti" sia uno dei consigli peggiori che si possa dare a un bambino. Moltissime persone sono disponibili e possono essere d'aiuto, e se un bambino si trova in qualche guaio, chiedere aiuto a uno sconosciuto è forse la cosa migliore che può fare.

Questo consiglio avrebbe aiutato Brennan Hawkins, il ragazzino di 11 anni disperso per quattro giorni nel deserto dello Utah il mese scorso. Egli evitava le persone che lo cercavano perché gli era stato insegnato di non parlare agli sconosciuti.

In un mondo dove le brave persone sono molte e i malintenzionati una minoranza, presumere che un qualsiasi sconosciuto sia una brava persona è una strategia di sicurezza intelligente. Dobbiamo aiutare i bambini a sviluppare i loro istinti naturali per quanto riguarda i rischi, e non regole così eccessivamente generiche.

Sempre in "Beyond Fear" ho scritto:

"Sia in quanto individui sia come società, possiamo effettuare delle scelte riguardo alla nostra sicurezza. Possiamo scegliere di avere più sicurezza o meno sicurezza. Possiamo scegliere di avere un maggior numero di imposizioni sulla nostra vita e sulla nostra libertà, oppure possiamo scegliere di avere meno imposizioni. Possiamo scegliere i tipi di rischio e di soluzioni di sicurezza che intendiamo tollerare e stabilire che altri siano inaccettabili.

"Come individui, possiamo decidere di acquistare un sistema d'allarme per la nostra casa che ci renda più sicuri, oppure possiamo risparmiare il denaro perché riteniamo che la sicurezza aggiunta non varrebbe il denaro speso. Possiamo decidere di non viaggiare per paura del terrorismo, o possiamo decidere di vedere il mondo perché è un luogo meraviglioso. Possiamo aver paura degli sconosciuti perché potrebbero essere degli aggressori, o possiamo parlare agli sconosciuti perché potrebbero diventare nostri amici".

<http://wireservice.wired.com/wired/story.asp?section=Breaking&storyId=1052553&tw=wn_wire_story> oppure <<http://tinyurl.com/b52ao>>

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

Commenti dei lettori

Da: "Richard M. Conlan" <kaige@embracetherandom.com>

Oggetto: Degli stupidi acquistano biglietti per un concerto falsificati

Nella sua analisi è insita la presupposizione secondo cui il sistema venga utilizzato esattamente come lei lo descrive. Nella pratica, ho acquistato e stampato biglietti online TicketMaster per diverse manifestazioni e, giunto sul luogo, i biglietti non sono MAI stati scansionati. Sapendo questo, molta gente si aspetta che anche un biglietto del bagarino possa andar bene ugualmente... Dipende dall'evento e dal luogo dell'evento. Ammetto che gli eventi a cui mi riferisco non sono necessariamente manifestazioni o spettacoli altisonanti in luoghi altrettanto altisonanti, ma il concetto rimane.

Sempre in argomento, continuo a chiedermi quanto difficile sarebbe per qualcuno scrivere un virus che controlli le caselle di posta su server POP in cerca di email che hanno "ticketmaster" nel campo "da:" e un allegato PDF, per poi spedire i PDF in un centro di raccolta.

Questo è particolarmente utile se un bagarino prende i biglietti, ne vende una copia e dice semplicemente agli acquirenti di arrivare presto sul luogo dell'evento (cioè prima dei legittimi possessori dei biglietti). In questo caso sarebbero i legittimi possessori del biglietto a vedersi negato l'accesso... oppure si ritroverebbero le vittime innocenti della frode sedute al loro posto.

Da: Paul Schumacher <psch@optonline.net>

Oggetto: Controlli ai raggi X? È solo l'inizio...

Utilizzare semplici raggi X per controllare se le persone sono armate o meno è soltanto l'inizio. Che cosa accadrà quando anche le volanti della polizia avranno questo equipaggiamento per controllare le persone in strada, alla ricerca di oggetti proibiti? Gli abiti con rivestimento in alluminio diventeranno di moda, per difendere la privacy, o saranno anch'essi vietati?

Ancora peggio è il radar a scansione terahertz. Come i raggi X a retrodiffusione, può vedere attraverso i vestiti. A differenza di essi, può vedere anche attraverso i muri. Già immagino furgoni della polizia pattugliare quartieri residenziali, effettuando "perquisizioni" nelle varie abitazioni senza nemmeno entrarvi. E potrebbero sostenere che non è necessario un mandato di perquisizione perché non occorre metter piede nella proprietà, né tantomeno in casa. Tutto questo, unitamente a computer dotati di riconoscimento d'immagine, può portare a una rapida ed efficace scansione e perquisizione di un'abitazione.

Le domande, a questo punto, sono:

1. Verrà dato il permesso alle forze dell'ordine di fare immediata irruzione e arrestare persone colte in flagrante con la scansione a raggi X, alla stessa stregua di quando la polizia osserva il compimento di un reato attraverso una finestra aperta?

2. Sarà permesso utilizzare questi metodi di scansione a raggi X (a retrodiffusione, terahertz) per perquisire virtualmente le persone in strada, in special modo senza esserne a conoscenza e senza il loro permesso?

3. Questo genere di prova sarà ammesso in tribunale, o sarà ammessa come ragione per ottenere un regolare mandato di perquisizione?

4. Sarà vietato l'uso pubblico di eventuali contromisure passive per contrastare questi metodi di scansione a raggi X (a retrodiffusione, terahertz), come avviene in molte zone per i giubbotti antiproiettile? (Esempi: abiti con rivestimento in alluminio, drappi alle finestre, pannelli isolanti di alluminio su muri e soffitto, finestre metallizzate o virtuali. ecc.)

Con le politiche anti-privacy dell'attuale amministrazione, vedo un'era in cui i nostri diritti del quarto emendamento rischiano di perdere di significato.

Negli anni Sessanta e Settanta del secolo scorso vi fu enorme scalpore in merito a basi dati informatiche del governo che raccoglievano informazioni sugli individui, e il Congresso le dichiarò virtualmente illegali. Oggi sono comuni e diffuse quanto gli scarafaggi in un tugurio. Questa tecnologia avrà il medesimo spaventoso impatto nella nostra vita quotidiana.

Da: "Thomas Bryce, M.D." <bryce@miyako.org>

Oggetto: Ridotta all'osso la legge sulla privacy sanitaria statunitense

Lei ha scritto: "L'industria della sanità si è opposta alla HIPAA fin dal principio, perché impone limiti ai suoi affari in nome della sicurezza e della privacy".

Molti medici generici come me sono contrari alle parti della HIPAA (che è una legge abbastanza esaustiva che affronta un gran numero di questioni) riguardanti le informazioni protette non perché imponga limiti agli affari, ma semplicemente perché non è compito del governo regolare il flusso di informazioni mediche.

La pratica medica e la protezione dei pazienti sono sempre state questioni di competenza dei singoli stati, e le norme della HIPAA sulla privacy non sono altro che un tentativo da parte di Washington di continuare a insinuarsi e ad estendere la propria autorità e influenza per coprire ogni aspetto del governo del nostro paese.

Al di là del fatto che non è compito del governo federale regolare la pratica medica, la HIPAA è semplicemente... una stupidata. Le norme sono assurdamente restrittive e inammissibili per nessuna ragione giustificabile. Per esempio, la HIPAA ha la pretesa (ritengo la HIPAA incostituzionale e dunque non valida -- ecco perché dico "ha la pretesa di") di vietare a un medico di dare informazioni su un paziente a terze parti tranne quando è il paziente stesso ad acconsentire oppure in determinate circostanze.

Ciò significa che se un medico riceve la telefonata di un parente del paziente che chiede informazioni sullo stato di salute del paziente, il medico non potrà fornire alcuna

informazione a meno che il paziente non abbia dato in precedenza il suo esplicito consenso.

Questo è (1) semplicemente ridicolo. Il medico dovrebbe affidarsi al proprio giudizio della situazione medica e alle caratteristiche/gravità della stessa, nonché sulle proprie conoscenze del paziente e dei familiari, e quindi determinare se sia o meno appropriato parlare con quel membro della famiglia. E (2) anche se non fosse ridicolo, semplicemente non sono affari del governo federale. Questo genere di cose viene regolato a livello dei singoli stati.

Da: Jeff Bee <jeff.bee@sbcglobal.net>
Oggetto: Il rischio dei coltelli appuntiti

In quanto falegname, ingegnere e conoscitore di buoni coltelli e utensili affilati in generale, posso individuare alcuni dei motivi della permanenza di estremità appuntite nelle lame più lunghe. In quello che ritengo un ordine di efficacia decrescente, le ragioni sono:

1. Aspettative del cliente. Lo stesso motivo che porta a produrre intenzionalmente aspirapolvere più rumorosi del necessario. La gente inconsciamente mette in proporzione l'efficacia dell'aspirapolvere con il rumore che esso produce, e se lei dà una matita ad un acquirente e chiede di disegnare un coltello, tutti tenderanno a disegnare un'estremità appuntita. Che questo sia un invito all'uso potenziale dei coltelli come armi d'attacco, o una dimostrazione della passività della percezione del pubblico può essere oggetto di un'altra discussione.

2. Meccanica dell'equilibrio. La maggioranza degli utenti si trova a proprio agio con una lama che presenta un punto di equilibrio (più esattamente, come diciamo noi del mestiere, il centro del momento inerziale) vicino al punto di transizione fra impugnatura e lama. Se una lama è più lunga dell'impugnatura a cui è attaccata, il modo più semplice per mantenere un corretto equilibrio è quello di affusolare la lama. Se una lama si assottiglia in spessore, il design intuitivo impone che essa debba assottigliarsi anche in larghezza, mantenendo un "allungamento alare" relativamente costante in sezione trasversale. Il risultato è una punta.

3. Meccanica dei tagli curvi. Il raggio minimo di un taglio curvo concavo che può essere prodotto da un coltello è limitato dalla larghezza della lama. Per trarne la massima utilità, una qualche parte della lama dovrebbe essere molto stretta se si intende effettuare dei tagli curvi. La meccanica dei materiali impone che tale parte ristretta deve trovarsi all'estremità di una lama affusolata; in altre parole, deve terminare in una punta.

4. Meccanica del taglio di lame in movimento. Lame che vengono realizzate per essere usate in modo dinamico, o fatte roteare, come un machete, possono effettivamente necessitare di una punta per una miglior efficacia. Come saprà, spesso un taglio a incisione (come per affettare) è più efficace del forzare una lama in un materiale perpendicolarmente allo spigolo. Vi sono due ragioni che spiegano questo, ma non entrerò nei dettagli in questa sede; basti sapere che per ottenere tale movimento di taglio in una lama in moto o in rotazione, lo spigolo tagliente viene inclinato verso la

direzione di moto. Il risultato può essere una lama ricurva, come nella scimitarra, o più comunemente, una lama lunga e appuntita. Ciò non si applica ai coltelli da cucina, perché molti di essi non vengono lanciati, mentre le mannaie sono fatte per tagliare a colpi, incuneando la lama, poiché il taglio a incisione non ha effetto su materiali rigidi come l'osso.

Quando sono in giro, porto sempre dei coltelli addosso. Di solito ho anche con me qualche tipo di pinza, una torcia, una penna; in altre parole, utensili. Il mio coltello principale è un serramanico con lama tanto da 3.95" assicurato alla mia tasca, e a volte è visibile. Di tanto in tanto mi viene chiesto il motivo per cui porto un'arma con me, e devo spiegare quanto segue:

Non ho mai usato (e spero di non dover usare mai) un coltello come arma di difesa né tantomeno come arma di attacco, per il semplice fatto che un coltello è un'arma efficace in pochissime situazioni dove in genere si ha un elemento di sorpresa e si intende bloccare l'avversario o più probabilmente ucciderlo. Non vado certo a mettermi in simili situazioni.

La situazione in cui è più probabile che io venga a trovarmi è quella di un'aggressione generata da violenza o dall'intento di derubarvi. In tale situazione non intendo uccidere nessuno, ma solo bloccare momentaneamente o rallentare l'avversario quanto basta per poter fuggire, un compito davvero inadatto per un coltello. Ferite da trafittura o lacerazioni prodotte da un taglio non bloccano nessuno a meno di non essere accuratamente mirate, e lasciandomi con un aggressore ancora più infuriato, una lama appuntita e precaria in mano, e molto probabilmente con accuse di aggressione armata.

Non ritengo che la disponibilità di coltelli appuntiti sia da inserirsi nella stessa categoria di sicurezza delle rivoltelle per due motivi. Primo, lunghi coltelli a punta hanno molti più usi legittimi che solo la difesa o l'attacco. Secondo, l'efficacia dei coltelli a punta, o dei coltelli in genere, deriva direttamente dalle capacità e dalla forza di chi li usa. Le armi da fuoco derivano la propria efficacia da energia chimica in esse conservata e non richiedono quasi alcuna abilità per generare una forza distruttiva.

Alla fin fine, i rischi di sicurezza non sono insiti negli strumenti che una persona utilizza per attaccare gli altri, ma nelle intenzioni di chi li maneggia. Se priviamo di un certo strumento un individuo intenzionato e motivato, egli ne sceglierà un altro. Da un punto di vista matematico si può considerarla un'iterazione senza fine. Pertanto dovremmo cercare di limitare le cause del dolo e la vulnerabilità agli attacchi invece di agire sui soli strumenti di attacco.

Da: Rob Isaac <rob@automagic.org>

Oggetto: Il rischio dei coltelli appuntiti

Perché i coltelli a lama lunga sono appuntiti? Per ragioni di ingegneria meccanica, di efficacia dei costi, e di tradizione.

I coltelli europei a lama lunga vengono tradizionalmente costruiti con un semplice sistema di asportazione -- lo spigolo affilato viene creato rimuovendo smerigliando

progressivamente il metallo finché non viene raggiunta la forma della lama. I coltelli hanno un'estremità appuntita perché è più semplice ottenere quella forma quando si rettifica lo spigolo in una curva.

Vi è anche una questione di costi, perché anche se la punta di un coltello a lama lunga viene raramente usata per trafiggere qualcosa in ambito culinario, la superficie tagliente viene utilizzata in tutta la lunghezza della lama che ovviamente termina in una punta. Se volete realizzare un coltello privo dell'ultimo centimetro di spigolo affilato, allora occorre allungare tutto il coltello di un centimetro per ottenere la stessa utilità. Il metodo di asportazione richiede dunque che si parta con un pezzo di acciaio di maggiori dimensioni.

L'aspetto legato alla tradizione è ovvio. I coltelli di ogni tipo sono tutti evoluzioni di idee progettuali che hanno migliaia di anni, e le impressioni della gente su che forma debba avere un coltello e su come debba essere utilizzato non sono così facili da cambiare. Non è stato universalmente stabilito alcun limite oltre il quale un coltello è considerato troppo lungo per essere usato allo scopo di trafiggere o tagliare. Quando la maggioranza dei più conosciuti coltelli da cucina di alta qualità e prodotti in serie a livello mondiale viene realizzata da più di trecento anni nello stesso gruppo di cittadine tedesche, e la gente continua a comprare quei coltelli, non c'è questo grande incentivo a cambiarne la formula.

Da: Anonimo

Oggetto: La pubblica divulgazione della perdita di dati personali

Bruce, i suoi commenti sulla perdita di dati sono azzeccati. Sì, è accaduto per anni e anni e sì, la sensibilità del pubblico verso tali perdite finirà con l'affievolirsi.

La sua chiosa è stata "La divulgazione pubblica è una buona cosa, ma non è sufficiente". La risposta alla sua domanda implicita su come possiamo risolvere questo pasticcio, a mio avviso risiede in una supervisione da parte dei regolatori. Moltissime società che hanno visto la divulgazione pubblica della loro perdita di informazioni sensibili sono organizzazioni di servizi finanziari governate da regolatori. Dietro le quinte, i regolatori stanno mettendo bene in chiaro come siano insoddisfatti dagli attuali livelli di controllo su informazioni personalmente identificabili e si aspettano cambiamenti significativi. Le compagnie regolamentate stanno rispondendo perché devono farlo.

Quelle compagnie che hanno subito perdite di dati, ma che non sono regolate (come ChoicePoint) chiaramente non vogliono che tali incidenti le facciano finire sulla lista governativa degli enti regolamentati. Questo offre un netto incentivo alle compagnie non regolamentate per mettere in atto dei cambiamenti.

L'altra forza motrice in atto è l'outsourcing. Nessun paese sostiene il lavoro in outsourcing verso altri paesi e si servirà di ogni pretesto per prevenire o limitare la perdita di posti di lavoro. Un argomento che sta ricevendo parecchia attenzione al Congresso è che le compagnie di outsourcing offshore sono dotate di scarse misure di sicurezza e presentano un grave rischio di perdita di informazioni. Che questo argomento sia fondato o no, sta attirando un supporto significativo da parte del pubblico. Qualsiasi compagnia che dipende in larga misura dall'outsourcing offshore della processazione di

informazioni sensibili è cosciente del rischio potenziale che il governo possa imporre seri limiti sul movimento dei dati verso l'estero e sa che deve agire in modo da garantire al pubblico la protezione dei loro dati. In moltissimi casi, se la compagnia trova dei metodi di protezione dei dati nel muoversi verso l'estero, essa sarà in grado di usare le medesime procedure in ambito domestico.

Non sono preoccupato del fatto che le compagnie statunitensi comprendano il messaggio. Quel che più mi preoccupa è se saranno in grado di trovare delle soluzioni con sufficiente rapidità così da poter affrontare il problema con efficienza ed efficacia. Perché se non ci riescono, allora dovremo comprare un bel po' di materiale della Brinks.

Da: "Nick Swift" <nick@swift.me.uk>
Oggetto: REAL ID

In risposta a questo messaggio di Petri Aukia sui documenti di identità:
"Vi è una sottile differenza, da lei non menzionata, fra le patenti di guida americane ed europee e le loro conseguenze sulla privacy.

Le patenti finlandesi e francesi (e molto probabilmente tutte le altre della Comunità Europea) non riportano l'indirizzo di casa del conducente. Servono a documentare la tua esistenza, il tuo nome, la tua foto, la tua firma, il numero di previdenza sociale, e il tipo di veicoli che sei abilitato a guidare. Pittogrammi, numeri e disposizioni dei dati sono standardizzati, per cui un agente di pattuglia può leggere la patente di guida di qualsiasi nazione della UE.

Ogni paese ha un meccanismo per far derivare l'indirizzo del conducente dal numero di previdenza sociale o da un dato equivalente, ma questo è a disposizione solo del governo e delle aziende a cui tu hai dato la possibilità di conoscere il tuo indirizzo (giornali, riviste, e simili)".

Le patenti di guida del Regno Unito mostrano l'indirizzo del conducente -- è la voce n.8 nel modello di patente europea. Questa voce è facoltativa, ma appare in molte patenti con fototessera, come in questo documento sulla Spagna.

<http://europa.eu.int/comm/transport/home/drivinglicence/legislation/doc/2003_10_22_memo_drivinglicence_en.pdf> oppure <<http://tinyurl.com/55xkw>>

I requisiti effettivi per una patente di guida sono esposti qui:

<http://europa.eu.int/eur-lex/en/consleg/pdf/1991/en_1991L0439_do_001.pdf> oppure <<http://tinyurl.com/8lcc7>>

Da notare che il numero di Previdenza Sociale non è un elemento richiesto obbligatoriamente come parte della patente.

Da: Brad Knowles <brad@stop.mail-abuse.org>
Oggetto: REAL ID

Nella sezione "Commenti dei lettori", Julien Maisonneuve ha detto: "In aggiunta a quanto da lei accennato in merito alle strutture legali europee atte a proteggere i dati sensibili (che non sono affatto complete e predominanti attraverso la comunità come uno vorrebbe), la stessa nozione di "furto d'identità" è pressoché sconosciuta in Europa. Vi sono molte cause, molte legate ai benefici assai limitati che uno può ottenere dall' "identità" in sé. Ciò include l'assenza di posizione creditizia esistente negli USA, e procedure diverse per l'apertura di conti bancari e di ottenimento dell'accesso alle loro risorse".

Vi sono altri effetti collaterali della questione. Per esempio, conoscere il numero di conto corrente bancario di una persona è sufficiente per poter inviare denaro a quella persona, ma non per sottrarlo. Molte società espongono i propri numeri di conto corrente persino sulla carta intestata e in molti li fanno stampare sui propri biglietti da visita. Non comporta alcun rischio il fatto che questa informazione venga "rubata" perché le banche non permettono di ritirare denaro sapendo soltanto il numero di conto corrente, e ciò semplifica il trasferimento di denaro per via elettronica. Questo, in larga misura, è alla base del motivo per cui in Europa non si fa quasi più uso di assegni -- è più facile e veloce trasferire denaro per via elettronica.

D'altro canto, cercare di impostare un pagamento per via elettronica verso conti correnti statunitensi è una pena. Ho provato a farlo attraverso la mia banca. Se hanno già una registrazione dell'azienda in questione, ci possono volere solo due o tre mesi per implementare addebiti e accrediti per via elettronica. Non è così complicato e faticoso in Europa.

Molte banche europee creano il proprio software personalizzato per l'intera gestione dell'internet banking, e questo software non solo girerà su Windows ma anche Macintosh e Linux. Tale software, sia in modalità offline sia online, permette di fare tutto quello che normalmente si fa andando a un bancomat o a una filiale della banca.

C'è un altro effetto collaterale -- le banche europee e le istituzioni di credito finanziario non convalidano le carte di credito online. Esiste invece una procedura manuale che impiega ore o giorni per processare le informazioni, spesso richiedendo interventi manuali e l'uso di fax. Questo rende molto difficoltoso lo shopping online quando il commerciante richiede una convalida online, ed è impossibile utilizzare qualunque negozio online dove la convalida online sia l'unica possibilità di scelta.

Anche se sono carte di credito Visa e hanno stampato il logo e l'ologramma Visa, non vengono riconosciute come carte Visa perché le prime cifre della carta indicano che non sono state rilasciate a un'istituzione bancaria USA. Se prendete macchine a noleggio da Avis, basta dire loro che l'indirizzo del noleggiatore è oltreoceano, e potrete noleggiare un veicolo con una carta di debito, cosa che normalmente non permettono.

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

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

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

La versione italiana è curata da Communication Valley SpA

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

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

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

Per informazioni crypto-gram@communicationvalley.it.

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

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

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

Copyright (c) 2005 by Bruce Schneier.