

CRYPTO-GRAM
15 dicembre 2006

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:

Rivotare
Le password del mondo reale
Le ristampe di Crypto-Gram
Seguire le tracce di qualcuno attraverso le sue scarpe da ginnastica
Frode notarile
News
La separazione della proprietà dei dati e della proprietà dei dispositivi
Le news di BT Counterpane
Combattere le transazioni fraudolente
Allarme cyber-crimine: molti sensazionalismi
Commenti dei lettori

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

Rivotare

Nel mondo elettorale, leggi sul riconteggio automatico non sono infrequenti. Un esempio è lo stato della Virginia, dove George Allen ha perso contro James Webb nella corsa al Senato per 1.800 voti su un totale di più di 2,3 milioni di voti (ossia per uno scarto dello 0,33%). Se il margine di vittoria è minore o uguale all'un percento, il candidato perdente può richiedere un riconteggio. Se il margine è minore o uguale allo 0,5%, il governo pagherà; se è compreso fra lo 0,5% e l'1%, sarà il candidato perdente a pagare le spese del riconteggio.

I riconteggi esistono perché il conteggio dei voti è, per usare un eufemismo, approssimativo. Agli americani piace avere i risultati delle elezioni il più presto possibile, prima di andare a dormire al termine della giornata elettorale. Pertanto siamo disposti a sorvolare sulle varie imprecisioni nelle procedure di conteggio e ignorare il fatto che i numeri che poi vediamo apparire alla televisione non riflettono la realtà delle cose in maniera molto precisa.

Tradizionalmente questo ha sempre avuto poca importanza, poiché molti errori di voto erano "errori casuali".

Esistono due tipologie essenziali di errori di voto: errori casuali ed errori sistemici. Gli errori casuali sono, appunto, casuali, e possono capitare a chiunque con uguale probabilità. In gare elettorali serrate gli errori casuali non cambiano di molto i risultati, perché i voti a favore del candidato A attribuiti per errore al candidato B sono probabili quanto i voti a favore di B attribuiti per errore ad A (da un punto di vista matematico, all'aumentare del margine di vittoria del candidato A, gli errori casuali tendono a ridurlo leggermente).

Questo è il motivo per cui, storicamente, è assai raro che i riconteggi in gare elettorali serrate finiscano col cambiare il risultato. Il riconteggio rivelerà una minima percentuale di errori in entrambe le direzioni, e si annulleranno a vicenda. Ma in una gara elettorale molto serrata, un attento riconteggio darà un risultato differente, ma è un caso piuttosto raro.

L'altra tipologia di errore di voto è l'errore sistemico, ovvero errori nel processo di voto (nelle macchine, nelle procedure), che fanno in modo che i voti a favore di A saranno attribuiti a B secondo un rapporto diverso rispetto alla situazione opposta.

Un esempio di questo genere di errore può essere una macchina per il voto elettronico che misteriosamente registrasse più voti per A di quanti siano gli elettori (un caso purtroppo non infrequente con le macchine per il voto elettronico). Un altro esempio può essere un errore casuale che accade soltanto con le attrezzature per il voto utilizzate in zone in cui A riceve un forte sostegno. Gli errori sistemici possono costituire un'enorme differenza in un'elezione, perché possono facilmente spostare migliaia di voti da A a B senza che vi sia alcuno spostamento da B ad A a ristabilire un equilibrio.

Ancora peggio, gli errori sistemici possono introdurre errori totalmente sproporzionati a ogni reale casualità nel processo di conteggio dei voti. In altre parole, la vicinanza di un'elezione non diviene affatto indicativa dell'eventuale presenza o assenza di errori sistemici.

Quando un candidato ha le prove della presenza di errori sistemici, un riconteggio può sistemare un risultato errato, ma solamente se durante il riconteggio è possibile scovare l'errore. Con le macchine per il voto elettronico troppo spesso non ci sono nemmeno dati su cui lavorare, e quindi non ci sono voti da riconteggiare.

Le elezioni avvenute quest'anno nel 13esimo Collegio Elettorale della Florida ne sono un esempio: il vincitore ha vinto con un margine di 373 voti su un totale di 237.861, ma almeno 18.000 voti non sono stati registrati dalle macchine per il voto elettronico. Quei voti provenivano da zone in cui il candidato perdente veniva favorito rispetto al vincitore, e avrebbero molto probabilmente ribaltato i risultati.

Oppure immaginiamo questa ipotetica situazione (ipotetica per quanto ne sappiamo): dopo le elezioni, viene scoperto del software malevolo nelle macchine per il voto che ha cambiato alcuni voti per il candidato A in voti per B. Oppure qualcuno viene scoperto mentre sta manomettendo i voti, modificando i dati delle schede di memoria elettroniche. Il problema in questi casi è che il voto originario è perduto per sempre, e tutto quel che abbiamo è il voto modificato.

Di fronte a questi problemi, possiamo scegliere una delle due seguenti alternative: attestare comunque il risultato, consci che purtroppo le persone sono state private di un loro diritto, ma altrettanto

consapevoli che non è possibile riparare quel torto. Oppure possiamo comunicare agli elettori di ritornare alle urne.

Senza dubbio, la sola idea di rivotare è già problematica in sé. Le elezioni sono un'istantanea, fermano un momento particolare nel tempo (la giornata elettorale) e il tornare a votare non rifletterà tale concetto. Se lo stato della Virginia avesse rivotato per il Senato quest'anno, l'elezione non avrebbe riguardato soltanto il ruolo di junior senator della Virginia, ma il controllo dell'intero Senato. Analogamente, nelle elezioni presidenziali in Florida dell'anno 2000, o nelle elezioni presidenziali in Ohio dell'anno 2004, i voti in seconda battuta dei singoli stati avrebbero deciso la presidenza.

E a chi si dovrebbe permettere di rivotare? Dovrebbero rivotare solo le persone nei distretti in cui vi sono stati dei problemi, oppure bisognerebbe rifare daccapo le elezioni? In ogni caso è certo che un maggior numero di elettori andrà a votare, magari cambiando le statistiche di affluenza e indirizzando i risultati in una direzione diversa rispetto al primo insieme di elettori. È questa una cosa negativa o positiva?

Dovrebbero rivotare solo le persone che possono provare di avere già votato (i registri vengono conservati) o che possono dimostrare di essere state allontanate dai seggi per errore? In questo caso, la seconda votazione avrà quasi certamente un minor numero di elettori, dato che alcuni degli elettori originari non avranno la possibilità di votare una seconda volta. E questo è probabilmente un male, o forse non lo è.

L'unica analogia di cui disponiamo in merito sono le elezioni di spareggio, che sono obbligatorie in alcune giurisdizioni nel caso in cui il candidato vincitore non ha ottenuto il 50% dei voti. Ma è facile sapere quando è necessario organizzare una votazione di spareggio. Chi decide, e in base a quali prove, che è necessario rivotare?

Ammetto di non avere risposte a riguardo. È necessario fermarsi ed esaminare attentamente le elezioni e ciò che vogliamo ottenere. Ma una sicurezza intelligente in ambito elettorale non solo cerca di prevenire sabotaggi dei voti (o anche gli errori sistemici delle macchine per il voto elettronico), ma organizza procedure di recupero e ripristino dopo che un'elezione è stata inquinata. Dobbiamo cominciare a discutere tali problematiche adesso, finché si trovano in un terreno neutrale, invece di attendere sviluppi inevitabili e le linee di battaglia già tracciate e imposte da quei risultati.

Florida 13:

<<http://www.heraldtribune.com/apps/pbcs.dll/article?AID=/20061111/NEWS/611110643>> oppure <<http://tinyurl.com/ygo731>>
<<http://www.nytimes.com/2006/11/10/us/politics/10florida.html>>

<<http://www.newsbackup.com/about496345.html>>

Questo articolo è originariamente apparso su Wired.com.

<<http://www.wired.com/news/columns/0,72124-0.html>>

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

Le password del mondo reale

Quanto sono valide le password che le persone scelgono per proteggere i propri computer e i propri account online?

È una domanda a cui è molto difficile rispondere, data la scarsità di dati a riguardo. Ma recentemente un mio collega mi ha inviato alcuni estratti risultanti da un attacco di phishing ai danni di MySpace: 34.000 nomi utente e password reali.

L'attacco è stato piuttosto elementare: gli aggressori hanno creato una finta pagina di login di MySpace e hanno raccolto le informazioni di login di quegli utenti che erano convinti di accedere ai propri account su quel sito. I dati sono stati inoltrati a una serie di server Web compromessi, dai quali gli aggressori li avrebbero raccolti in un secondo momento.

Secondo le stime di MySpace, più di 100.000 persone sono state vittime dell'attacco prima che fosse bloccato. I dati in mio possesso provengono da due punti di raccolta diversi, e sono stati ripuliti della piccola percentuale di persone che hanno capito di star rispondendo a un attacco di phishing. Ho analizzato i dati, e ne ho dedotto quanto segue.

Lunghezza delle password: se il 65% delle password contiene otto caratteri o meno, il 17% è costituito da sei caratteri o meno. La lunghezza media di una password è di otto caratteri.

Nello specifico, la distribuzione della lunghezza delle password è la seguente:

1-4 caratteri: 0.82%
5 caratteri: 1.1%
6 caratteri: 15%
7 caratteri: 23%
8 caratteri: 25%
9 caratteri: 17%
10 caratteri: 13%
11 caratteri: 2.7%
12 caratteri: 0.93%
13-32 caratteri: 0.93%

Sì, vi è una password lunga 32 caratteri: "lancheste23nite4lancheste23nite4". Altre password lunghe sono "fool2thinkfool2thinkol2think" e "dokitty17darling7g7darling7".

Composizione delle password: se l'81% delle password sono alfanumeriche, il 28% sono composte semplicemente da lettere minuscole e una cifra finale, e per i due terzi di tale percentuale quella cifra è 1. Solo un 3,8% delle password sono una parola intera presente nel dizionario, e un altro 12% è costituito da password composte da una parola del dizionario più una cifra finale; ancora una volta, per i due terzi di tale percentuale la cifra è 1.

Solo numeri: 1,3%
Solo lettere: 9,6%
Alfanumeriche: 81%
Non-alfanumeriche: 8,3%

Solo lo 0,34% degli utenti ha utilizzato la porzione del nome utente del proprio indirizzo email come password.

Password più comuni: le 20 password più usate sono (nell'ordine): password1, abc123, myspace1, password, blink182, qwerty1, fuckyou, 123abc, baseball1, football1, 123456, soccer, monkey1, liverpool1, princess1, jordan23, slipknot1, superman1, iloveyou1 e monkey.

La password più comune in assoluto, "password1", è stata usata per lo 0,22% di tutti gli account. Dopodiché la frequenza diminuisce rapidamente: "abc123" e "myspace1" sono state impiegate soltanto nello

0,11% di tutti gli account, "soccer" [gioco del calcio] nello 0,04% e "monkey" [scimmia] nello 0,02%.

Per chi non lo sapesse, Blink 182 è un gruppo musicale. Presumibilmente molte persone utilizzano il nome di quel gruppo perché contiene numeri, e quindi sembra un'ottima password. Il gruppo Slipknot non ha numeri nel proprio nome, e questo spiega il numero "1" aggiunto in coda. La password "jordan23" fa riferimento al giocatore di basket Michael Jordan e al suo numero di maglia. E, naturalmente, "myspace" e "myspace1" sono password facili da ricordare per un account MySpace. Non capisco invece che cosa c'entrino le scimmie.

Eravamo soliti scherzare dicendo che "password" è la password più comune. Adesso è "password1". Chi ha detto che gli utenti non hanno imparato nulla sulla sicurezza?

Battute a parte, le password stanno migliorando. Sono impressionato dal fatto che meno del 4% delle password erano parole del dizionario e che la stragrande maggioranza erano almeno alfanumeriche. Nel 1989 Daniel Klein fu in grado di craccare il 24% delle sue password di esempio con un piccolo dizionario di soli 63.000 termini, e scoprì che la lunghezza media delle password era di 6,4 caratteri.

E nel 1992 Gene Spafford ha craccato il 20% delle password con il suo dizionario, e ha scoperto che la lunghezza media delle password era di 6,8 caratteri. (Entrambi hanno studiato password Unix, che all'epoca avevano una lunghezza massima di otto caratteri). Ed entrambi hanno riportato una percentuale molto maggiore di password con caratteri tutti minuscoli, e password tutte minuscole con l'iniziale maiuscola, rispetto ai dati emersi dal caso MySpace. Il concetto di scegliere buone password sta cominciando ad attecchire, almeno in minima parte.

D'altro canto il campione demografico di MySpace è piuttosto giovane. Un altro studio sulle password condotto a novembre ha esaminato 200 password di impiegati di azienda: il 20% composte da sole lettere, il 78% alfanumeriche, il 2,1% con caratteri non-alfanumerici e una lunghezza media di 7,8 caratteri. Meglio rispetto a 15 anni fa, ma non agli ottimi livelli degli utenti di MySpace. I giovani sono davvero il nostro futuro.

Niente di tutto questo però cambia il fatto che l'utilità delle password come serio strumento di sicurezza è sorpassata da un pezzo. Nel corso degli anni, i cracker di password sono diventati sempre più veloci. Gli attuali prodotti in commercio possono verificare decine, anche centinaia di milioni di password al secondo. Allo stesso tempo esiste un livello massimo di complessità per memorizzare una password da parte dell'utente medio. I limiti oltrepassati anni fa, e le tipiche password del mondo reale, oggi sono indovinabili dai software. Il Password Recovery Toolkit di AccessData, al ritmo di 200.000 tentativi al secondo, avrebbe potuto craccare il 23% delle password di MySpace in 30 minuti, e il 55% in otto ore.

Ovviamente questa analisi presuppone che l'aggressore possa impadronirsi del file con la password criptata e lavorarci sopra offline, a suo piacimento; ovvero nel caso in cui la stessa password sia stata usata per criptare un'email, un file o un disco rigido. Le password possono ancora funzionare se si riescono a evitare attacchi offline, e si fa attenzione a eventuali attacchi online. Inoltre vanno bene in quelle situazioni di sicurezza di basso valore, o nel caso si utilizzino password davvero complesse e software come Password Safe per conservarle. Per il resto, una sicurezza basata sulle sole password è piuttosto rischiosa.

L'attacco a MySpace:

http://www.infoworld.com/infoworld/article/06/10/27/HNphishingmyspace_1.html oppure <http://tinyurl.com/y29f81>
<http://news.netcraft.com/archives/2006/10/27/myspace_accounts_compromised_by_phishers.html> oppure <http://tinyurl.com/yggk83>
<<http://www.securiteam.com/securitynews/6000M0AHFW.html>>

Un'altra analisi degli stessi dati:

<http://www.infoworld.com/article/06/11/17/470Psecadvise_1.html>

Altri studi sulle password:

<http://www.deter.com/unix/papers/passwords_klein.ps.gz>
<<http://ftp.cerias.purdue.edu/pub/papers/gene-spafford/spaf-OPUS-observe.pdf>> oppure <http://tinyurl.com/y815vm>
<http://www.fredstie.com/thesis/survey/survey_report.pdf>
<<http://download.lawr.ucdavis.edu/pub/CambridgePWStudy.pdf>>

Password cracking:

<<http://www.lockdown.co.uk/?pg=combi&s=articles>>
<<http://www.accessdata.com/products/decryption/>>

Password Safe:

<<http://passwordsafe.sourceforge.net/>>

Questo articolo è originariamente apparso su Wired.com.

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

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

Le ristampe di Crypto-Gram

Crypto-Gram è attualmente al suo nono 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).

La sicurezza aerea:

<<http://www.schneier.com/crypto-gram-0512.html#1>>

Il rootkit DRM di Sony:

<<http://www.schneier.com/crypto-gram-0512.html#6>>

Sorveglianza e supervisione:

<<http://www.schneier.com/crypto-gram-0512.html#10>>

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

<<http://www.schneier.com/crypto-gram-0412.html#1>>

Kafka e la Persona Digitale:

<<http://www.schneier.com/crypto-gram-0412.html#8>>

Per un uso sicuro del personal computer:

<<http://www.schneier.com/crypto-gram-0412.html#10>>

Blaster e il black-out del 14 agosto:

<<http://www.schneier.com/crypto-gram-0312.html#1>>

Crittografia quantica:

<<http://www.schneier.com/crypto-gram-0312.html#6>>

Il voto computerizzato ed elettronico
<<http://www.schneier.com/crypto-gram-0312.html#9>>

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

Osservazioni sul Dipartimento per la Sicurezza Nazionale
<<http://www.schneier.com/crypto-gram-0212.html#3>>

Il crimine, ovvero la prossima grande novità di Internet
<<http://www.schneier.com/crypto-gram-0212.html#7>>

Documenti d'identità nazionali:
<<http://www.schneier.com/crypto-gram-0112.html#1>>

I giudici puniscono le pessime misure di sicurezza:
<<http://www.schneier.com/crypto-gram-0112.html#2>>

Sicurezza informatica e responsabilità:
<<http://www.schneier.com/crypto-gram-0112.html#4>>

Farsi beffe degli scanner di vulnerabilità:
<<http://www.schneier.com/crypto-gram-0112.html#9>>

Le votazioni e la tecnologia:
<<http://www.schneier.com/crypto-gram-0012.html#1>>

"La Sicurezza non è un Prodotto; è un Processo":
<<http://www.schneier.com/crypto-gram-9912.html#1>>

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

Gli algoritmi digitali cellulari europei:
<<http://www.schneier.com/crypto-gram-9912.html#10>>

L'inutilità delle gare di cracking:
<<http://www.schneier.com/crypto-gram-9812.html#contests>>

Come riconoscere il testo in chiaro (plaintext):
<<http://www.schneier.com/crypto-gram-9812.html#plaintext>>

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

Seguire le tracce di qualcuno attraverso le sue scarpe da ginnastica

Dei ricercatori dell'Università di Washington hanno dimostrato un sistema di sorveglianza che traccia automaticamente le persone attraverso il kit Nike+iPod. Sostanzialmente, il kit contiene un trasmettitore da inserire nelle scarpe da ginnastica e un ricevitore da collegare all'iPod. Ciò permette di registrare tempi, distanze, ritmo e calorie bruciate. Molto interessante.

Tuttavia pare che il trasmettitore nelle scarpe da ginnastica possa essere letto fino a una ventina di metri di distanza. E dato che trasmette un ID unico, è possibile essere rintracciati grazie a esso. Nella dimostrazione, i ricercatori hanno costruito un dispositivo di sorveglianza (del costo di circa 250 dollari) e lo hanno interfacciato con Google Maps. Spaventoso.

È una bella dimostrazione per chiunque non creda che sia possibile

C'è ancora tempo per inviare studi.

<http://weis2007.econinfosec.org/>

Molte storie riguardanti la TSA questo mese. La prima: un passeggero innocente arrestato per aver cercato di portare una pallina elastica a bordo di un aereo.

<http://www.flyertalk.com/forum/showthread.php?t=618629>

La seconda: una donna è svenuta su un aereo dopo che le sue droghe sono state confiscate.

<http://www.thelocal.se/5493/20061113/>

La terza: gli screener del San Francisco International Airport sono stati avvertiti in anticipo di un test che sarebbe stato condotto a loro insaputa.

<http://sfgate.com/cgi-bin/article.cgi?f=/c/a/2006/11/17/BAG72MESP91.DTL>

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

La quarta: salsa per spaghetti surgelata quasi sequestrata.

<http://www.salon.com/tech/col/smith/2006/11/22/askthepilot210/>

Abbiamo un grave problema in questo paese. La TSA opera al di sopra e al di là della legge. Non vi è alcun giusto processo, nessuna revisione giudiziaria, nessun appello.

E una vignetta sulla TSA:

<http://www.gocomics.com/thefifthwave/2006/11/19/>

Sei iman musulmani sono stati allontanati da un volo della US Airways perché... beh, perché sono musulmani e questo spaventa la gente. Dopo essere stati rilasciati dalle autorità, la US Airways si è rifiutata di vendere loro un biglietto aereo.

<http://www.startribune.com/462/story/826056.html>

<http://www.tcdailyplanet.net/node/2963>

Si noti che il colpevole qui è la US Airways, non la TSA. Non lasciatevi terrorizzare!

<http://www.schneier.com/essay-124.html>

Un articolo interessante sulla storia e sull'attuale ricerca di una droga che spinge le persone a dire la verità:

<http://www.washingtonpost.com/wp-dyn/content/article/2006/11/19/AR2006111900891.html> oppure <http://tinyurl.com/w9mgp>

David Kahn dona la sua biblioteca di criptologia al National Cryptologic Museum a Fort Meade, Maryland:

<http://www.nytimes.com/2006/11/23/arts/23arts.html>

Qualche settimana fa a Seattle è stata organizzata un'esercitazione di bioterrorismo. Vari corrieri hanno recapitato finti pacchi a "praticamente migliaia" di persone (sì, questo è quanto riporta l'articolo; a mio parere si tratta di "circa un migliaio" di persone), verificando come il sistema postale possa essere utilizzato per distribuire rapidamente medicine. Certo, vi sono molti contesti in cui questo genere di sistema di distribuzione non sarebbe sufficientemente adeguato, ma non è questo il punto. In generale, ritengo che la risposta nei casi di emergenza sia una delle poche aree in cui è necessario investire più denaro. E penso che collaudi ed esercitazioni come questa siano una buona cosa: in quali altri modi possiamo sapere se i sistemi funzioneranno come vogliamo che funzionino?

http://www.king5.com/localnews/stories/NW_110906WABbioterrordrillKC.205f0d23.html

<http://www.metrokc.gov/health/postaldelivery/index.htm>

<http://alexfandra.livejournal.com/107641.html>

La scorsa settimana, l'Ufficio Copyright degli Stati Uniti ha rilasciato

un nuovo elenco di esenzioni alla DMCA.

<http://www.copyright.gov/1201/>

<http://www.freedom-to-tinker.com/?p=1090>

<http://www.businessweek.com/ap/financialnews/D8LIEI500.htm>

Truffa dell'inchiostro cancellabile: una persona va di porta in porta, richiedendo contributi per un'istituzione benefica. Come metodo di pagamento preferisce l'assegno: dopotutto è il sistema più sicuro per voi. Ma per compilare l'assegno e firmarlo vi offre la sua penna, e la penna contiene inchiostro cancellabile. Di seguito, corregge sia il beneficiario dell'assegno sia la cifra, e va a incassarlo. Questo tipo di truffa non è affatto nuovo, ovviamente, ma sta accadendo oggi nel Regno Unito. Ho già avuto occasione di parlare di aggressori che utilizzano diversi solventi per cancellare l'inchiostro degli assegni, ma questo trucco è ancora più elementare: è l'aggressore stesso a offrire alla vittima una penna alterata. Credevo che gli assegni fossero stampati con un inchiostro che fosse anch'esso cancellabile, rendendo così nullo un assegno modificato. Perché questo genere di attacco funziona ancora?

http://iccroydon.icnetwork.co.uk/news/headlines/tm_headline=-magic-ink--conmen-fleece-cash-donors&method=full&objectid=18151895&siteid=53340-name_page.html

oppure <http://tinyurl.com/vc5mp7>

http://www.schneier.com/blog/archives/2006/02/check_washing.html

Per sedersi e ordinare frittelle è necessario un documento con foto:

http://www.redorbit.com/news/oddtities/746680/ihop_changes_policy_of_asking_for_ids/index.html?source=r_oddtities

oppure <http://tinyurl.com/ya6no8>

Il Dipartimento per la Sicurezza Nazionale vuole condividere le informazioni biometriche dei terroristi con altri paesi, in un programma chiamato "Global Envelope". Qualcuno pensa che sarà migliore della no-fly list?

http://www.gcn.com/online/voll_no1/42677-1.html?topic=authentication&CMP=OTC-RSS

oppure <http://tinyurl.com/w85bw>

Esiste un nuovo software che si dice sia in grado di predire chi ha più probabilità di diventare un assassino. Il tutto è piuttosto inquietante, dato che si spinge nell'ambito dello psicoreato.

<http://www.philly.com/mld/philly/news/local/16104571.htm?template=contentModules/printstory.jsp>

oppure <http://tinyurl.com/yygj4f>

In segreto e nel corso di questi ultimi anni, gli agenti di immigrazione hanno assegnato a chiunque entrasse o lasciasse il paese un profilo di rischio terroristico generato da un computer. Come sempre con questi sistemi, tutti veniamo giudicati in segreto, da un algoritmo di un calcolatore, senza la possibilità di esaminare o discutere il nostro profilo di rischio. Kafka sarebbe orgoglioso. Una citazione dalla storia dell'Associated Press: " 'Se questo serve a catturare anche un solo potenziale terrorista, si tratta di un successo', ha dichiarato Ahern". È un'affermazione talmente idiota che non vale nemmeno la pena di replicare.

http://news.yahoo.com/s/ap/20061201/ap_on_go_ca_st_pe/traveler_screening_6

oppure <http://tinyurl.com/ylnab6>

<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>

Commenti:

<http://www.epic.org/privacy/surveillance/spotlight/1006/default.html>

http://digbysblog.blogspot.com/2006_12_01_digbysblog_archive.html#116497716038834002

oppure <http://tinyurl.com/y88lnr>

La comunicazione del Federal Register:

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

I commenti alla comunicazione:

http://www.epic.org/privacy/pdf/ats_comments.pdf
http://www.eff.org/Privacy/ats/ats_comments.pdf
<http://www.aclu.org/privacy/gen/275931eg20061201.html>

La prova che il programma è illegale:

<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://hasbrouck.org/IDP/IDP-ATS-comments.pdf>
<http://www.ledger-enquirer.com/mld/ledgerenquirer/news/local/16196947.htm> oppure <http://tinyurl.com/y7lbnp>
<http://www.chron.com/disp/story.mpl/ap/politics/4387187.html>

Il Congresso ha passato una legge anti-pretexing. Non arriva al punto di alcune leggi statali, sulle quali si impone, ma è sempre un'ottima cosa.

<http://arstechnica.com/news.ars/post/20061211-8395.html>

In precedenza, la MPAA aveva fatto sopprimere una legge anti-pretexing della California, affermando che aveva dovuto commettere una frode per fermare i download illeciti. Il mio commento all'epoca: queste persone sembrano sempre più un'organizzazione criminale.

<http://www.wired.com/news/technology/0,72214-0.html>

"Un uomo di nazionalità rumena è stato accusato di hacking ai danni di più di 150 computer del governo statunitense, provocando sconvolgimenti che sono costati alla NASA, al Dipartimento dell'Energia e alla Marina quasi un milione e mezzo di dollari". Era da molto che non leggevo notizie come questa.

<http://www.cnn.com/2006/TECH/12/01/hacker.charged.ap/index.html>

Tengo una conferenza dal titolo "The Future of Privacy" [Il Futuro della Privacy], in cui parlo degli sviluppi tecnologici odierni e futuri che erodono la nostra privacy. Una di queste tecnologie è l'intercettazione uditiva, e ipotizzo che il microfono di un telefono cellulare potrebbe essere attivato a distanza e di nascosto. Non ho mai avuto prove vere e proprie a riguardo, ma tale tecnica è emersa durante il processo contro un reato organizzato. Pare che la tecnica consista nello scaricare software di intercettazione nel telefono.

http://news.zdnet.com/2100-1035_22-6140191.html

<http://www.nj.com/news/ledger/index.ssf?/base/news-10/1165815713294600.xml&coll=1> oppure <http://tinyurl.com/y36o9d>

Storia interessante di una giornalista inglese che ha comprato 20 passaporti europei falsi. Ha acquistato un vero passaporto ceco con un falso nome e con la sua vera foto, un passaporto lettone fasullo, e un passaporto estone rubato. Si noti che i passaporti RFID, più difficili da contraffare, sarebbero d'aiuto solo in un caso; di certo non è il problema più importante da risolvere.

http://news.bbc.co.uk/2/hi/uk_news/6169678.stm

Ho già trattato in precedenza della tecnologia a raggi X a retrodiffusione. È ottima per scovare armi nascoste indosso a una persona, ma è altrettanto ottima per vedere una persona completamente nuda. La TSA sta collaudando questa tecnologia a Phoenix, e stanno deliberatamente sfocando le immagini per proteggere la privacy. Da notare che il sistema viene migliorato rendendo le immagini risultanti meno dettagliate. Eccellente.

<http://www.tsa.gov/research/privacy/backscatter.shtm>

http://www.schneier.com/blog/archives/2005/06/backscatter_x-r.html

URL del post nel mio blog:

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

Questo è interessante. Ted Kaczynski (Unabomber) scriveva in codice. Si trattava di un cipher scritto a matita su carta che il governo

(l'articolo dice "la CIA", ma presumibilmente era la NSA a essere coinvolta) non ha potuto decodificare finché qualcuno non ha trovato la chiave fra le carte di Kaczynski. Qualcuno conosce i dettagli dell'algoritmo?

http://cbs5.com/topstories/local_story_332014518.html

http://cbs5.com/slideshows/local_slideshow_332010422/view?slide=7

Sono il primo ad ammetterlo: non so quasi niente di siti come MySpace o Facebook. So che si tratta di siti di social networking e che, in certa misura, la reputazione di un membro si basa su chi sono i suoi "amici" e su ciò che essi dicono di lui. E, come la notte segue il giorno, ecco "Fake Your Space": un sito in cui è possibile incaricare falsi amici affinché lascino la loro fotografia e dei commenti personalizzati nel vostro spazio. Ora è possibile far finta di essere più popolari di quanto lo si è in realtà. Che cosa si inventeranno poi? Servizi che verificano gli amici sulle vostre pagine degli amici di MySpace? Servizi che bloccano i servizi di verifica degli amici? Dove andrà a finire tutto questo?

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

Nota: probabilmente si tratta di un sito-burla.

Le banche stanno investendo milioni per evitare che degli outsider rubino le identità dei loro clienti, ma esiste una crescente minaccia di attacchi dall'interno.

http://news.com.com/2100-1029_3-6137940.html

Un attacco molto furbo ai danni delle tessere regalo. Il truffatore prende le tessere non attive dagli espositori nei negozi e copia i numeri di serie. Poi, una volta online, va a verificare se è stata attivata qualche tessera. In caso positivo, inizia a fare spese folli.

<http://www.startribune.com/535/story/857643.html>

Qual è il problema di sicurezza? Un numero di serie sulle tessere visibile anche quando una tessera non è attiva. Si potrebbe mitigare il rischio nascondendo il numero seriale dietro un rivestimento da grattare oppure usando un involucre opaco per avvolgere la tessera.

Uno studio assolutamente affascinante su un firewall RFID personale. L'idea di fondo è quella di portare con voi un dispositivo personalizzato che dirotta i segnali di tutti i tag RFID sulla vostra persona finché non lo autorizzate a fare diversamente. Hanno persino costruito un prototipo. Come fa notare Cory Doctorow, questo è potenzialmente un sistema per godere dei benefici del RFID senza dover pagarne i costi.

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

http://www.cs.vu.nl/~melanie/rfid_guardian/papers/lisa.06.pdf

http://www.boingboing.net/2006/12/06/personal_firewall_fo.html

Si tratta di una storia bizzarra, che riguarda "la radice quadrata dell'intento terroristico". Appare in una equazione che determina quanto denaro federale ricevono varie strutture locali per la difesa antiterrorismo.

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

http://public.cq.com/public/20061204_homeland.html

Ho scritto un articolo sullo spam per il sito Forbes.com.

http://www.forbes.com/security/2006/12/11/spam-security-email-tech-security-cz_bs_1212spam.html oppure <http://tinyurl.com/y6a63u>

In esso non vi è molto che non abbia già detto in precedenza.

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

<http://www.schneier.com/crypto-gram-0402.html#9>

Un altro articolo sullo spam:

<http://www.freedom-to-tinker.com/?p=1094>

Degli hacker hanno avuto accesso a un database contenente informazioni personali di 800.000 fra studenti ed ex-studenti dell'UCLA. Quasi non vale la pena di trattare simili eventi: si tratta dell'ennesimo attacco ai danni di un database con la conseguente esposizione di informazioni personali. Immagino che ogni cittadino americano ormai sia stato vittima di almeno un attacco di questo genere. Ma una parte dell'articolo ha attratto la mia attenzione: "Jim Davis, vice-rettore associato per l'information technology dell'UCLA, ha definito l'attacco molto sofisticato: ha utilizzato un programma progettato per sfruttare la vulnerabilità di una singola applicazione software fra le centinaia usate in tutto il Westwood campus. 'Un aggressore ha scoperto una piccola falla ed è stato in grado di servirsene, per poi coprire le proprie tracce', ha affermato Davis". Mi preoccupa il fatto che il vice-rettore associato per l'information technology non si renda conto che TUTTI gli attacchi funzionano in quel modo.

<http://www.latimes.com/news/local/la-me-ucla12dec12,0,7111141.story>

Il rapporto del CATO sul data mining e il terrorismo. Da leggere assolutamente:

http://www.cato.org/pub_display.php?pub_id=6784

Ingannare le porte difese da un sensore di movimento usando un bastone. Un vecchio trucco, ma un'ottima storia:

<http://thedailywtf.com/forums/thread/106137.aspx>

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

La separazione della proprietà dei dati e della proprietà dei dispositivi

Considerate due diversi problemi di sicurezza. Nel primo caso, conservate i vostri oggetti di valore in una cassaforte nel vostro seminterrato. La minaccia è rappresentata dai ladri, ovviamente. Ma la cassaforte è proprietà vostra, e la casa pure. Avete il controllo degli accessi alla cassaforte, e probabilmente avete predisposto un sistema d'allarme.

Il secondo caso è simile, solo che i vostri valori vengono conservati nella cassaforte di qualcun altro. Ancora peggio, si tratta di qualcuno di cui non vi fidate. Questa persona non conosce la combinazione, ma controlla gli accessi a essa. Può cercare di forzarla come gli pare, prendendosi tutto il tempo necessario. Può trasportare la cassaforte in qualunque posto desideri. Può utilizzare qualsiasi strumento egli preferisca. Nella prima situazione la cassaforte deve rimanere al sicuro, ma è sempre solo una parte della vostra sicurezza domestica. Nel secondo caso, la cassaforte è l'unico dispositivo di sicurezza che avete.

Questo secondo problema di sicurezza può sembrare un po' artificioso e forzato, a prima vista, ma è una cosa che accade regolarmente nella nostra società dell'informazione: i dati controllati da una persona vengono conservati in un dispositivo controllato da un'altra. Si pensi a quelle smart card prepagate: se la persona che possiede la tessera riesce a romperne la sicurezza, può aggiungere denaro alla carta. Si pensi a un sistema DRM: la sua sicurezza si poggia sul fatto che chi possiede il computer non è in grado di accedere al sistema di sicurezza DRM. Si pensi al chip RFID di un passaporto. O a una macchina affrancatrice. O al traffico SSL inviato attraverso una rete pubblica.

Questi sistemi sono difficili da proteggere, e non solo per il fatto che si affida il dispositivo all'aggressore e gli si permette di utilizzare tutto il tempo e ogni strumento e capacità necessari per forzarlo. La

protezione è ardua perché in genere quando la sicurezza viene compromessa, si tratta di "class break". L'esperto che trova il modo di distruggere il sistema di sicurezza può costruire hardware, o scrivere software, che lo faccia automaticamente. Basta una persona per distruggere un dato sistema DRM; il software può forzare ogni altro dispositivo appartenente alla stessa classe.

Ciò significa che la sicurezza non deve solo difenderci dall'aggressore medio, ma dall'aggressore più intelligente, più motivato e meglio finanziato.

Mi è tornato alla mente questo problema agli inizi del mese, quando dei ricercatori hanno annunciato un nuovo attacco contro le implementazioni del criptosistema RSA. L'attacco si serve del fatto che diverse operazioni necessitano di tempi differenti nelle moderne CPU. Controllando attentamente, e attivamente influenzando la CPU durante un'operazione RSA, un aggressore può recuperare la chiave. Le applicazioni più ovvie di tale attacco vengono svolte ai danni di quei sistemi DRM che cercano di utilizzare una partizione protetta della CPU per evitare che il proprietario del computer possa ricavare le chiavi crittografiche del sistema DRM stesso.

Questo genere di attacchi non è nuovo. Nel 1995 dei ricercatori scoprirono che era possibile recuperare chiavi crittografiche confrontando i tempi relativi sui chip. Negli anni successivi, sia la corrente che le radiazioni sono stati utilizzati per rompere i criptosistemi. Ho definito tali attacchi "side-channel" perché fanno uso di altre informazioni oltre che il testo in chiaro e il testo cifrato. E per quali applicazioni si rivelano molto utili? Per recuperare segreti dalle smart card.

Ogni volta che vedo sistemi di sicurezza caratterizzati da questa separazione dati/dispositivi, cerco di risolvere il problema di sicurezza eliminando la separazione, e ciò significa ridisegnare completamente il sistema e le assunzioni di sicurezza che stanno dietro.

Si confronti una smart card prepagata con una carta di debito. Nel primo caso, il proprietario della carta può creare denaro cambiando il valore della carta. Perché tale sistema sia sicuro, la smart card deve essere protetta da una serie di misure di sicurezza. Nel secondo caso non vi è alcun segreto nella carta. Alla banca non importa che si possa leggere il numero stampato sulla carta, o i dati ricavabili dalla banda magnetica sul retro. I veri dati, e la sicurezza, stanno nei database della banca.

Oppure si confronti un sistema DRM con un modello finanziario che non si cura della copia. Il primo è impossibile da proteggere, il secondo è assai più facile.

Benché sia molto diffuso nei sistemi digitali, questo tipo di problema di sicurezza non si limita a essi. Lo scorso mese, la provincia di Ontario ha avviato un'indagine sulle frodi interne ai suoi sistemi di lotteria "gratta e vinci", dopo che la CBC ha insinuato che chi vende i biglietti è in grado di capire quali siano i biglietti vincenti e non li vende. È lo stesso problema: i proprietari dei dati sui biglietti (la commissione della lotteria) ha cercato di mantenere i dati segreti proteggendoli da chi aveva accesso fisico ai biglietti, e hanno fallito.

Si confronti tutto questo con un sistema tradizionale di lotteria a estrazione settimanale. L'attacco non è possibile, perché il biglietto non nasconde alcun segreto da scoprire.

Separare la proprietà dei dati e la proprietà dei dispositivi non implica l'impossibilità di applicare una sicurezza: è solo molto più

<http://www.schneier.com/news-022.html>

Podcast:

Sono stato intervistato in merito ai passaporti RFID:

http://digitaldebateblogs.typepad.com/digital_identity/2006/11/bruce_schneier_.html oppure <http://tinyurl.com/yxdx37>

Gary McGraw mi ha intervistato per il suo podcast "Silver Bullet Security":

<http://www.cigital.com/silverbullet/show-009/>

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

Combattere le transazioni fraudolente

Lo scorso marzo ho scritto che l'autenticazione a due fattori non servirà a ridurre le frodi finanziarie o i furti di identità, che tutto quel che farà sarà obbligare i criminali a cambiare tattica. Questo è quanto sostenevo alcuni mesi fa:

"Purtroppo, la tipologia degli attacchi è cambiata in questi vent'anni. Ai tempi, le minacce erano soltanto passive: intercettazioni e tentativi di scoperta delle password effettuati offline. Oggi le minacce sono decisamente attive: phishing e cavalli di Troia.

"Ecco due nuovi attacchi attivi che si iniziano ad incontrare:

"- Attacco di tipo Man-in-the-Middle: un aggressore realizza un finto sito Web di una banca e spinge l'utente verso quel sito. L'utente inserisce la sua password e l'aggressore la sfrutta per accedere al vero sito della banca. Se questo attacco viene ben architettato, l'utente non si accorgerà di non essere nel vero sito Web della sua banca. Poi l'aggressore scollegherà l'utente e farà tutte le transazioni fraudolente che vuole, oppure permetterà all'utente di fare le proprie transazioni insieme alle sue transazioni illegali, nel medesimo tempo.

"- Attacco Trojan: l'aggressore installa un Trojan nel computer dell'utente. Quando l'utente si autentica al sito Web della banca, l'aggressore sfrutta il Trojan per inserirsi in remoto nella stessa sessione, in modo da fare tutte le transazioni fraudolente che vuole.

"Vedete come l'autenticazione a due fattori non risolve niente? Nel primo caso, l'aggressore può passare la parte sempre variabile della password alla banca insieme alla parte fissa. Nel secondo caso l'aggressore si affida all'utente per autenticarsi".

La soluzione non è quella di migliorare l'autenticazione dell'utente, ma di autenticare la transazione. (Si pensi alle carte di credito. Nessuno controlla la vostra firma. A nessuno importa che voi siate davvero voi. Le compagnie di carte di credito mantengono la sicurezza autenticando le transazioni.)

Naturalmente nessuno mi ascolta. I regolatori negli Stati Uniti hanno richiesto alle banche di implementare l'autenticazione a due fattori entro la fine di quest'anno. Ma i clienti si stanno opponendo, e le banche stanno facendo di tutto per inventarsi qualcos'altro, qualsiasi cosa. E la cosa sorprendente è che, apparentemente per puro caso, hanno trovato delle soluzioni di sicurezza che funzionano davvero. Da CSO:

"Invece, per conformarsi alle nuove regolamentazioni bancarie e arginare le perdite causate dal phishing, le banche e i loro fornitori stanno imbastendo in fretta e furia delle strategie multilivello allo scopo di costituire una autenticazione "forte". L'approccio emergente in genere

consiste nel riconoscere in qualche modo il computer di un cliente, nel proporre domande aggiuntive che rivelino un eventuale comportamento rischioso e implementando sistemi back-end antifrode.

[...]

“Malgrado le indicazioni FFIEC sull'autenticazione, le tecnologie emergenti che sembrano più promettenti per proteggere i fondi nei conti correnti bancari non sono affatto i sistemi di autenticazione. Sono invece sistemi back-end che rilevano eventuali comportamenti sospetti.

“Alcuni di questi strumenti si basano su regole: se un cliente del Nebraska entra nel sistema autenticandosi, per esempio, dalla Romania, la banca può stabilire che quel login venga sempre considerato sospetto. Altri sono basati su un punteggio di rischio: quel login dalla Romania aggiungerà punti a un profilo di rischio, e quando tale profilo raggiunge una certa soglia, la banca passa all'azione.

“Le transazioni segnalate come sospette possono essere dirottate verso un sistema di autenticazione a due fattori: solitamente una telefonata, qualcosa che l'utente possiede. Nella realtà delle carte di credito questo viene fatto manualmente da molto tempo. Si pensi all'ultima chiamata ricevuta dal dipartimento antifrode della vostra compagnia di carta di credito quando voi (o qualcun altro) avete provato a fare un grosso acquisto con la carta di credito in Europa. Alcune banche, fra cui la Washington Mutual, sono in procinto di automatizzare chiamate fuori banda in caso di transazioni online rischiose”.

Proprio così. Questo è ciò che occorre fare.

L'articolo di CSO:

http://www.csoonline.com/read/110106/fea_strong_auth.html

Il mio articolo sull'autenticazione a due fattori:

http://www.schneier.com/blog/archives/2005/03/the_failure_of.html

Il mio articolo sull'attenuazione del furto di identità:

http://www.schneier.com/blog/archives/2005/04/mitigating_iden.html

Le banche che hanno l'obbligo di implementare l'autenticazione a due fattori:

http://www.schneier.com/blog/archives/2005/10/us_regulators_r.html

Un altro esempio:

http://www2.csoonline.com/blog_view.html?CID=27198

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

Allarme cyber-crimine: molti sensazionalismi

Pare che sia la stagione dei sensazionalismi sul cyber-crimine. Abbiamo anzitutto un articolo della CNN, che non riporta nulla di nuovo:

“Gli esperti di sicurezza prevedono che gli hacker informatici apriranno un nuovo fronte nella 'guerra cibernetica' multimiliardaria nel 2007, prendendo di mira telefoni cellulari, servizi di messaggia istantanea e comunità Web come MySpace.

“Gli utenti si lasciano ingannare sempre meno dalle truffe via email, e quindi le bande criminali troveranno altri sistemi per commettere frodi online, vendere merci fasulle o rubare segreti aziendali”.

Poi abbiamo un articolo della BBC che sostiene che le organizzazioni criminali stanno finanziando gli studenti affinché ottengano diplomi e lauree IT:

"Le organizzazioni criminali di maggior successo si basano su partnership fra chi è dotato di esperienza e contatti nel mondo della criminalità e chi possiede le capacità tecniche, ha dichiarato il sig. Day.

" 'I criminali tradizionali possono disporre i loro fondi e utilizzare tutto il background di cui dispongono', ha detto, 'ma non hanno le adeguate conoscenze tecniche'.

"Con l'aumentare del numero di organizzazioni criminali che tentano di spostarsi nel cyber-crimine, è diventato sempre più difficile arruolare hacker esperti, ha affermato Day. Questo ha portato i criminali a prendere di mira gli studenti universitari di tutto il mondo.

" 'Alcuni studenti vengono finanziati durante la loro carriera accademica informatica, fino al conseguimento del diploma', ha affermato Day. Una volta diplomati, i ragazzi vanno a lavorare presso quelle organizzazioni criminali.

[...]

"L'aura di ribellione evocata da tale attività ha aiutato i criminali ad adescare ragazzi molto giovani, perfino quattordicenni, ha suggerito lo studio.

"Pescando fra siti web, forum e chat room che offrono strumenti di hacking, crack o password per software piratato, i reclutatori criminali raccolgono informazioni sui potenziali bersagli.

"Una volta identificati, i giovani hacker vengono attirati nel giro mediante ricompense per lavori a basso profilo, come utilizzare una rete di computer domestici compromessi, un botnet, o inviare spam.

"Il basso livello di rischio e le generose ricompense servono alle organizzazioni criminali per creare un'idea molto attraente di quella che può essere la vita di un criminale cibernetico, ha sostenuto Day.

"Con l'aumentare dei giovani attirati nella rete, la posta in gioco viene alzata sempre più, e ai ragazzi vengono affidati compiti sempre più rischiosi".

Criminali che prendono di mira dei ragazzini: ottimi ingredienti per far sensazione.

Intendiamoci, non è mia intenzione minimizzare la minaccia del cyber-crimine. Né voglio sottovalutare la minaccia del cyber-crimine organizzato. Un numero sempre maggiore di criminali sta affollando la rete, e il cyber-crimine si è spostato sempre più in alto nella catena alimentare, fino a consolidarsi in grandi associazioni di crimine organizzato. Il cyber-crimine è un grosso affare, e si sta ingrandendo sempre più.

Ma non so se storie come queste siano un bene o un male.

L'articolo della CNN:

<<http://www.cnn.com/2006/TECH/internet/12/12/cyber.crime.reut/index.html>

> oppure <<http://tinyurl.com/y6shu6>>

L'articolo della BBC:

<http://news.bbc.co.uk/2/hi/technology/6220416.stm>

** **

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) 2006 - Bruce Schneier.