

CRYPTO-GRAM  
15 gennaio 2008

Scritta da Bruce Schneier  
Fondatore e CTO di BT Counterpane

Edizione italiana curata da Communication Valley SpA  
<<http://www.communicationvalley.it/>>

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

Per consultare i numeri arretrati, o per iscriversi, andare all'indirizzo:  
<<http://www.schneier.com/crypto-gram.html>>.

Oppure si può leggere il presente numero direttamente sul Web, all'indirizzo:  
<<http://www.schneier.com/crypto-gram-0703.html>>.

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

Crypto-Gram è anche consultabile in formato RSS.

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

In questo numero:

- L'anonimato e il set di dati di Netflix
- News
- "Dove dovrebbe iniziare la sicurezza negli aeroporti?"
- Uno studio sulla sicurezza aeroportuale
- Le news su Schneier/BT Counterpane
- La mia rete wireless aperta
- Commenti dei lettori

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

L'anonimato e il set di dati di Netflix

L'anno scorso Netflix pubblicò le valutazioni di 10 milioni di film da parte di 500 mila clienti, come parte di una sfida per invitare il pubblico a proporre dei sistemi di segnalazione migliori di quello che la compagnia stava utilizzando. I dati furono poi resi anonimi eliminando informazioni personali e sostituendo i nomi con numeri casuali, per proteggere la privacy degli interessati.

Arvind Narayanan e Vitaly Shmatikov, ricercatori alla Università del Texas di Austin, hanno de-anonimizzato parte dei dati di Netflix confrontando le valutazioni e le indicazioni di data e ora con informazioni pubbliche presenti sull'Internet Movie Database (IMDb).

La loro ricerca dimostra alcuni problemi intrinseci delle informazioni anonime. Ma prima di tutto è importante spiegare ciò che i due ricercatori hanno fatto e quel che non hanno fatto.

NON hanno de-anonimizzato l'intero set di dati di Netflix. Il loro lavoro è stato quello di de-anonimizzare il set di dati di Netflix relativo soltanto a un campione di utenti che hanno inserito delle valutazioni sui film anche nell'IMDb, utilizzando i propri nomi. (Se da un lato gli archivi dell'IMDb sono pubblici, effettuare il crawling del loro sito per ottenerli è contrario ai termini del servizio di IMDb, pertanto i ricercatori si sono serviti di un piccolo campione rappresentativo per provare il loro algoritmo).

Lo scopo della ricerca era dimostrare come non siano necessarie molte informazioni per togliere l'anonimato ai dati presenti nel set di Netflix.

Da un certo punto di vista, non è forse ovvia una cosa del genere? Si è già parlato dei rischi dei database anonimi, come in uno studio del 2001 pubblicato in un periodico della IEEE. I ricercatori che hanno lavorato sui dati anonimi di Netflix non si sono messi a individuare meticolosamente l'identità dei singoli (come altri fecero con il database di ricerca di AOL lo scorso anno): li hanno soltanto confrontati con un subset di dati simili già identificato. Una tecnica standard del processo di data-mining.

Ma dato che le opportunità per effettuare questo genere di analisi spuntano sempre più di frequente, molte informazioni anonime potrebbero finire a rischio.

Per esempio, qualcuno che abbia accesso a un gruppo di dati anonimi di un registro telefonico potrebbe de-anonimizzarli parzialmente ponendoli in correlazione con il database telefonico di un catalogo di una società commerciale. Oppure le recensioni di libri sul sito di Amazon potrebbero essere la chiave per de-anonimizzare un database pubblico di acquisti con carta di credito, o un database più vasto di recensioni librerie anonime.

Google, grazie al suo enorme database contenente le ricerche effettuate dagli utenti in Internet, potrebbe facilmente togliere l'anonimato da un database di acquisti online, o concentrarsi sulle ricerche di termini medici per de-anonimizzare un database della salute pubblica. I commercianti che conservano informazioni dettagliate sui clienti e sugli acquisti potrebbero servirsi di quei dati per de-anonimizzare in parte qualunque insieme di informazioni di un motore di ricerca, se tali informazioni fossero pubblicate in forma anonima. Un data broker che mantiene i database di svariate aziende potrebbe essere in grado di togliere l'anonimato dalla stragrande maggioranza dei record di quei database.

Ciò che hanno dimostrato i ricercatori dell'Università del Texas è che tale procedimento non è per nulla difficile, e non necessita di molte informazioni. Si scopre che, una volta eliminati i cento film più visti dal pubblico, le nostre abitudini di consumatori di film sono tutte piuttosto individuali. Un discorso analogo si può certamente fare per le nostre abitudini di lettori, per le nostre abitudini di acquirenti online, per come utilizziamo il telefono, per le ricerche che effettuiamo sul Web.

Le ovvie contromisure per questo problema sono, purtroppo, inadeguate. Netflix avrebbe potuto randomizzare il proprio set di dati eliminando un subset, modificando le informazioni di data e ora oppure inserendo deliberatamente degli errori nei singoli numeri di identificazione utilizzati per sostituire i nomi. Si è scoperto, tuttavia, che

simili precauzioni rendono il lavoro di decodifica un po' più difficile, ma non di molto. L'algoritmo di de-anonizzazione di Narayanan e Shmatikov è sorprendentemente robusto e funziona con dati incompleti, dati che sono stati inquinati, persino dati contenenti errori.

Con soltanto otto valutazioni di film (delle quali due potrebbero essere totalmente errate), e date che possono essere sballate anche di due settimane, i due ricercatori riescono a identificare individualmente il 99 per cento dei record nel set di dati. Dopo di che, tutto quel che serve loro è qualche informazione identificabile: dall'IMDb, dal vostro blog, da qualsiasi fonte. La morale è che basta un piccolo database di nomi perché qualcuno possa scardinare l'anonimato di un database anonimo molto più vasto.

Altre ricerche arrivano alla medesima conclusione. Utilizzando informazioni pubbliche anonime del censimento del 1990, Latanya Sweeney ha scoperto che l'87 per cento della popolazione degli Stati Uniti, ossia 216 milioni di persone su 248 milioni, potrebbe essere singolarmente identificato mediante il codice di avviamento postale a cinque cifre, combinandolo con sesso e data di nascita. Circa la metà della popolazione degli Stati Uniti è teoricamente identificabile per sesso, data di nascita e città, paese o municipalità di residenza. Estendendo l'ambito geografico a un'intera contea riduce la percentuale a un comunque significativo 18 per cento. "In linea generale", hanno scritto i ricercatori, "sono necessarie poche caratteristiche per identificare un singolo individuo".

Dei ricercatori della Stanford University hanno riportato risultati molto simili servendosi delle informazioni del censimento del 2000. Si scopre che la data di nascita, che (a differenza del solo giorno e mese di nascita) ordina le persone in migliaia di gruppi differenti, è incredibilmente utile a disambiguare le persone.

Tutto ciò ha profonde conseguenze sulla pubblicazione di dati anonimi. Da una parte, le informazioni anonime rappresentano un grosso aiuto per i ricercatori: AOL ha fatto un'ottima cosa quando rilasciò il proprio set di dati anonimi a scopo di ricerca, ed è un peccato che a seguito delle proteste dell'opinione pubblica il CTO abbia dato le dimissioni e un intero team di ricerca sia stato licenziato. Grandi database di informazioni mediche sono estremamente preziosi per la società: per studi farmacologici su vasta scala, studi supplementari a lungo termine, e così via. Anche informazioni telefoniche anonime possono servire a compiere ricerche affascinanti.

D'altro canto però, nell'era della sorveglianza all'ingrosso, in cui tutti raccolgono continuamente informazioni su di noi, il processo di anonimizzazione è assai fragile e più rischioso di quel che può sembrare a prima vista.

Come ogni altra cosa in ambito di sicurezza, non si dovrebbero implementare sistemi di anonimato senza averli prima sottoposti ad attacchi avversari. Tutti sappiamo che è folle servirsi di un sistema crittografico prima che sia severamente collaudato sotto attacco. Perché dovrebbe essere diverso per i sistemi di anonimato? E, come ogni cosa legata alla sicurezza, anche l'anonimato è una serie di compromessi. Vi sono dei vantaggi e i corrispettivi rischi.

Narayanan e Shmatikov stanno attualmente lavorando allo sviluppo di algoritmi e tecniche che permettano la pubblicazione sicura di set di dati anonimi come quello di Netflix. È il risultato di una ricerca dalla quale tutti noi possiamo trarre beneficio.

<[http://www.cs.utexas.edu/~shmat/shmat\\_netflix-prelim.pdf](http://www.cs.utexas.edu/~shmat/shmat_netflix-prelim.pdf)>  
<<http://www.cs.utexas.edu/~shmat/netflix-faq.html>>  
<<http://www.securityfocus.com/news/11497>>  
<<http://arxivblog.com/?p=142>>

Lo studio del 2001 della IEEE:

<<http://people.cs.vt.edu/~naren/papers/ppp.pdf>>

Togliere l'anonimato ai dati di AOL:

<<http://query.nytimes.com/gst/fullpage.html?res=9E0CE3DD1F3FF93AA3575BC0A9609C8B63>>

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

<<http://www.securityfocus.com/brief/286>>

La de-anonimizzazione dei dati del censimento:

<<http://privacy.cs.cmu.edu/dataprivacy/papers/LIDAP-WP4abstract.html>>

<<http://crypto.stanford.edu/~pgolle/papers/census.pdf>>

Informazioni anonime di telefonia cellulare:

<<http://arxivblog.com/?p=88>>

La sorveglianza all'ingrosso e la raccolta dei dati:

<[http://www.schneier.com/blog/archives/2006/03/the\\_future\\_of\\_p.html](http://www.schneier.com/blog/archives/2006/03/the_future_of_p.html)>

<[http://www.schneier.com/blog/archives/2007/05/is\\_big\\_brother\\_1.html](http://www.schneier.com/blog/archives/2007/05/is_big_brother_1.html)>

Questo articolo è originariamente apparso su Wired.com.

<[http://www.wired.com/politics/security/commentary/securitymatters/2007/12/securitymatters\\_1213](http://www.wired.com/politics/security/commentary/securitymatters/2007/12/securitymatters_1213)>

oppure <<http://tinyurl.com/2gkl8a>>

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

## News

Microsoft ha aggiunto il generatore di numeri casuali Dual\_EC-DRBG a Windows Vista, come parte del Service Pack 1. Sì, proprio lo stesso generatore che potrebbe avere una backdoor della NSA. Non è abilitato per default, e non è chiaro se l'utente possa attivarlo. È eseguibile come chiamata di programma. Il mio consiglio è quello di non utilizzarlo. Mai.

<<http://technet2.microsoft.com/WindowsVista/en/library/417467e7-7845-46d4-85f1-dd471fbc0de91033.msp?mfr=true>>

oppure <<http://tinyurl.com/3xtwq9>>

<<http://msdn2.microsoft.com/en-us/library/aa375534.aspx>>

Sulla backdoor:

<<http://www.schneier.com/essay-198.html>>

Questo programma imita un essere umano all'interno di una chat room, e cerca di ottenere informazioni personali. E io che pensavo che ELIZA facesse tanto Anni Sessanta.

<[http://www.news.com/8301-13860\\_3-9831133-56.html](http://www.news.com/8301-13860_3-9831133-56.html)>

La classifica delle 10 più grandi fughe di dati del 2007, secondo CSO Magazine:  
<<http://www2.csoonline.com/exclusives/column.html?CID=33366>>

Impressionante evasione di due detenuti che hanno rimosso la malta intorno a un blocco di calcestruzzo per poi sfondarlo, passare attraverso il buco, raggiungere il tetto, e quindi saltare verso la libertà. Sono stati nuovamente catturati.

<<http://www.cnn.com/2007/US/law/12/17/nj.jailbreak/index.html>>  
<[http://www.schneier.com/blog/archives/2007/12/prison\\_break.html](http://www.schneier.com/blog/archives/2007/12/prison_break.html)>

IEEE Spectrum ha un articolo in tre parti sui Taser e come funzionano. Una lettura interessante, ma è bene sapere che due degli autori hanno legami con produttori di Taser, pertanto occorre aspettarsi una trattazione di parte delle varie problematiche.

<<http://www.spectrum.ieee.org/dec07/5731>>  
<<http://www.spectrum.ieee.org/dec07/5731/2>>  
<<http://www.spectrum.ieee.org/dec07/5731/3>>

Un filmato sui Taser:

<<http://www.cbc.ca/canada/british-columbia/story/2007/11/14/bc-taservideo.html>>

Non so nulla delle politiche dell'organizzazione Downsize DC, ma posso certamente sostenere la loro campagna "I am not afraid" [Io non ho paura]. Credo che tutti noi, a prescindere dal paese in cui viviamo, dovremmo inviare una lettera come questa ai nostri funzionari eletti: "Non ho paura del terrorismo, e voglio che smettiate di essere terrorizzati a nome mio. Vi chiedo, per favore, di iniziare a ridurre la guerra al terrore che ha intrapreso il governo. Sostituirela con un lavoro antiterroristico delle forze di polizia meno dispendioso e più concentrato, che rientri nella legge. Per favore, basta con le reazioni esagerate. Mi rendo conto che non sarà possibile fermare tutti gli atti terroristici. Lo accetto. Io non ho paura".

<<http://action.downsizedc.org/wyc.php?cid=77>>

Rifutate di farvi terrorizzare, e neutralizzerete l'arma più potente in mano ai terroristi: la vostra paura.

<[http://www.schneier.com/blog/archives/2006/08/what\\_the\\_terror.html](http://www.schneier.com/blog/archives/2006/08/what_the_terror.html)>

C'è anche questo video:

<<http://www.youtube.com/watch?v=ka5FdP-gNF0>>

Chicago apre un nuovo fronte alla guerra all'imprevisto, cercando di terrorizzare tutti:

<[http://www.schneier.com/blog/archives/2007/12/refuse\\_to\\_be\\_te.html](http://www.schneier.com/blog/archives/2007/12/refuse_to_be_te.html)>

La settimana scorsa, Ask.com ha annunciato una funzione chiamata AskEraser, che cancella la cronologia delle ricerche di un utente. È indubbiamente positivo vedere come le aziende si servano di funzionalità di privacy a scopi competitivi, tuttavia EPIC ha esaminato AskEraser e ha scritto all'azienda segnalando alcuni problemi.

<[http://www.schneier.com/blog/archives/2007/12/privacy\\_problem.html](http://www.schneier.com/blog/archives/2007/12/privacy_problem.html)>

Una vignetta sul furto d'identità:

<<http://www.dilbert.com/creators/speedbump/archive/images/speedbump2030558071218.gif>>

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

Un giudice federale del Vermont ha stabilito che la polizia non può costringere una persona a rivelare la propria chiave PGP. Ciò non porrà affatto termine al grande dibattito, ma sono certamente delle ottime novità.

<[http://www.news.com/8301-13578\\_3-9834495-38.html?tag=nefd.blgs](http://www.news.com/8301-13578_3-9834495-38.html?tag=nefd.blgs)>  
<[http://www.news.com/8301-13578\\_3-9835392-38.html?tag=nefd.blgs](http://www.news.com/8301-13578_3-9835392-38.html?tag=nefd.blgs)>  
<<http://yro.slashdot.org/article.pl?sid=07/12/15/1459243>>  
I commenti di Orin Kerr:  
<<http://volokh.com/posts/1197670606.shtml>>

Altre novità sulle macchine per il voto elettronico: dall'Ohio, dal Colorado e altrove:  
<[http://www.schneier.com/blog/archives/2007/12/more\\_voting\\_mac\\_1.html](http://www.schneier.com/blog/archives/2007/12/more_voting_mac_1.html)>

Babbo Natale e la TSA:  
<<http://images.ucomics.com/comics/nq/2007/nq071224.gif>>

Reality show televisivo "Tiger Team". Purtroppo non diventerà una serie.  
<[http://en.wikipedia.org/wiki/Tiger\\_Team\\_%28TV\\_series%29](http://en.wikipedia.org/wiki/Tiger_Team_%28TV_series%29)>  
<<http://www.trutv.com/video/?id=870&link=truTVshlk>>  
<<http://www.isohunt.com/torrents/%22tiger+team%22?iht=>>

Dipinti di Picasso rubati da un museo in Brasile:  
<<http://www.cnn.com/2007/WORLD/americas/12/20/brazil.heist.ap/index.html>>  
oppure <<http://tinyurl.com/337lxy>>  
<[http://www.schneier.com/blog/archives/2007/12/picasso\\_stolen.html](http://www.schneier.com/blog/archives/2007/12/picasso_stolen.html)>  
I dipinti sono stati ritrovati:  
<<http://www.foxnews.com/story/0,2933,321176,00.html>>

Un articolo sostiene che il software di back-end del 35% o dell'80-95% (a seconda di quale parte dell'articolo leggete) di tutti i siti Web per adulti sia stato compromesso, e che l'industria del porno stia passando il fatto sotto silenzio. Come molte altre storie di questo genere, non si hanno prove che gli aggressori siano in possesso del database di informazioni personali. La vulnerabilità significa solo che potrebbero averlo.  
<<http://www.icwt.us/index.php/2007/12/23/tens-of-thousands-of-adult-website-records-compromised/>>  
oppure <<http://tinyurl.com/3bu8bu>>  
<<http://it.slashdot.org/article.pl?sid=07/12/25/0050204>>

L'FBI sta realizzando un imponente database di dati biometrici. Visti i precedenti, c'è qualcuno che sia disposto a credere anche per un minuto che le proprie informazioni biometriche saranno sicure in questo database?  
<<http://www.washingtonpost.com/wp-dyn/content/article/2007/12/21/AR2007122102544.html>>  
oppure <<http://tinyurl.com/38f43s>>  
<<http://news.bbc.co.uk/go/rss/-/2/hi/americas/7158723.stm>>

A partire dal 2008 sono in vigore nuove norme per il trasporto di batterie al litio sugli aerei. Con buona approssimazione posso dire che gli unici a essere interessati da tali norme sono i professionisti dell'audio/video.  
<[http://www.schneier.com/blog/archives/2007/12/new\\_lithium\\_bat\\_1.html](http://www.schneier.com/blog/archives/2007/12/new_lithium_bat_1.html)>

Il worm/botnet Nugache, un'altra specie di malware.  
<[http://www.schneier.com/blog/archives/2007/12/the\\_nugache\\_wor.html](http://www.schneier.com/blog/archives/2007/12/the_nugache_wor.html)>

Questo filmato tratto dallo show australiano The Chasers sul terrorismo è di un paio di anni fa, ma non l'avevo mai visto prima. Divertente.

<<http://www.youtube.com/watch?v=W3grHjibNdA>>

Una foto divertente: "Un'accusa ingiusta":

<<http://i258.photobucket.com/albums/hh275/pizzler/sucks2bwronglyaccused.jpg>>

oppure <<http://tinyurl.com/2ebgg2>>

Articolo interessante sull'economia del cyber-crimine.

<<http://resources.zdnet.co.uk/articles/features/0,1000002000,39291463,00.htm>>

oppure <<http://tinyurl.com/yvzoe5>>

Il governo britannico cambia la propria retorica, dichiarando che la "guerra al terrore" è la maniera sbagliata di descrivere le cose:

<<http://www.military.com/NewsContent/0,13319,159067,00.html>>

"National Security for the Twenty-First Century" [Sicurezza Nazionale per il ventunesimo secolo] di Charlie Edwards, pubblicato da Demos, comitato di esperti inglese. È lungo (121 pagine) ma ricco di contenuti interessanti.

<<http://www.demos.co.uk/publications/nationalsecurityforthetwentyfirstcentury>>

oppure <<http://tinyurl.com/2vfqh8>>

Se vi unite alla "Comunità SHC" su Sears.com, la compagnia installerà spyware davvero potente sul vostro computer. Se questa fosse l'opera di un ragazzino con un temibile nome da hacker, verrebbe subito arrestato. Ma qui si tratta di Sears, per cui chissà come andrà a finire per loro. Ma quel che dovrebbe accadere è che le aziende anti-spyware cominciassero a trattare questo per il malware che è, e non ignorarlo perché proviene da un'azienda nella Fortune 500.

<<http://community.ca.com/blogs/securityadvisor/archive/2007/12/20/sears-com-join-the-community-get-spyware.aspx>>

oppure <<http://tinyurl.com/2ja6dr>>

Il profiling negli aeroporti, e gli arresti a cui ha portato:

<[http://www.schneier.com/blog/archives/2008/01/airport\\_behavior.html](http://www.schneier.com/blog/archives/2008/01/airport_behavior.html)>

Un buon articolo sui cospiratori di Fort Dix: le sfide derivanti dal perseguire il terrorismo in modo più fattivo e i rischi dell'utilizzo di informatori.

<<http://www.time.com/time/nation/article/0,8599,1691609,00.html>>

Ho trattato alcune di queste problematiche:

<<http://www.schneier.com/essay-174.html>>

Una vignetta sul "comportamento responsabile":

<<http://xkcd.com/364/>>

Un'altra vignetta divertente:

<<http://xkcd.com/350/>>

Un buon articolo del New York Times sulle macchine per il voto elettronico:

<<http://www.nytimes.com/2008/01/06/magazine/06Vote-t.html>>

L'esercito degli Stati Uniti sta installando computer Macintosh perché sono più difficili da hackerare:

<[http://www.forbes.com/home/technology/2007/12/20/apple-army-hackers-tech-security-cx\\_ag\\_1221army.html](http://www.forbes.com/home/technology/2007/12/20/apple-army-hackers-tech-security-cx_ag_1221army.html)>

oppure <<http://tinyurl.com/29xelf>>

Hackerare il Boeing 787. Pare che l'accesso Internet dei passeggeri possa essere collegato all'avioelettronica dell'aereo.

<[http://www.wired.com/politics/security/news/2008/01/dreamliner\\_security](http://www.wired.com/politics/security/news/2008/01/dreamliner_security)>

oppure <<http://tinyurl.com/2g3kj7>>

Ecco come la campagna "See Something, Say Something" [Se vedete qualcosa, dite qualcosa] funziona davvero: dati reali da New York.

<[http://www.schneier.com/blog/archives/2008/01/how\\_well\\_see\\_so.html](http://www.schneier.com/blog/archives/2008/01/how_well_see_so.html)>

Resoconto investigativo sulle frodi dei passaporti in tutto il mondo:

<<http://www.msnbc.msn.com/id/22419963/>>

Un articolo interessante sulla paura e il cervello:

<<http://www.newsweek.com/id/78178>>

Ho già scritto su questo genere di cose:

<<http://www.schneier.com/essay-155.html>>

L'esercito svedese smarrisce informazioni segrete conservate in una memory stick:

<<http://www2.mil.se/en/News/News/Misplaced-memory-stick-contained-classified-information/>>

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

Su questo tema sono intervenuto un paio di anni fa:

<<http://www.schneier.com/essay-105.html>>

<[http://www.schneier.com/blog/archives/2005/07/risks\\_of\\_losing.html](http://www.schneier.com/blog/archives/2005/07/risks_of_losing.html)>

Anche se non capisco assolutamente il motivo per cui l'esercito svedese non cripta i propri dispositivi portatili.

<[http://www.schneier.com/blog/archives/2007/12/how\\_to\\_secure\\_y.html](http://www.schneier.com/blog/archives/2007/12/how_to_secure_y.html)>

Da Privacy International, l'International Privacy Ranking [Valutazione della privacy internazionale] per il 2007:

<[http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-559597](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559597)>

oppure <<http://tinyurl.com/3bt4a4>>

Un bambino di cinque anni trattenuto dalla TSA perché il suo nome è simile all'alias di un sospettato terrorista. La spiegazione è semplice: per la TSA è più importante seguire le procedure che il buonsenso. Purtroppo, però, per acchiappare il prossimo terrorista sarà necessario servirsi più del buonsenso che seguire pedissequamente le procedure.

<<http://www.boingboing.net/2008/01/09/tsa-searches-detains.html>>

Pare che questo fosse in contrasto con la policy della TSA:

<[http://www.tsa.gov/approach/mythbusters/8yo\\_noflylist.shtm](http://www.tsa.gov/approach/mythbusters/8yo_noflylist.shtm)>

Resoconti dei clienti sulla sicurezza aerea e sulla TSA:

<[http://www.schneier.com/blog/archives/2008/01/consumer\\_report.html](http://www.schneier.com/blog/archives/2008/01/consumer_report.html)>

Questa vicenda, sulle backdoor della NSA inserite in macchine per la cifratura di Crypto AG, fece il giro dei giornali europei circa dieci anni fa (soprattutto notizie in tedesco, se non ricordo male), ma non se ne parlò molto qui negli Stati Uniti.

<<http://www.inteldaily.com/?c=169&a=4686>>

Patrick Smith sulla sicurezza aerea: un articolo eccellente dal blog sui viaggi del New York Times.

<<http://jetlagged.blogs.nytimes.com/2007/12/28/the-airport-security-follies/index.html>>

oppure <<http://tinyurl.com/26f69n>>

Business Week ha pubblicato un rapporto speciale sul Dipartimento per la Sicurezza Nazionale che comprende tre articoli diversi.

<[http://www.businessweek.com/technology/special\\_reports/20071217techhomelan.htm](http://www.businessweek.com/technology/special_reports/20071217techhomelan.htm)>

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

Paul Torrens, all'Arizona State University School of Geographical Sciences, possiede una simulazione computerizzata che si modella sul panico urbano:

<<http://pruned.blogspot.com/2007/06/modeling-urban-panic.html>>

Come imbrogliare a una prova d'esame sostituendo l'etichetta di una bevanda analcolica con una apparentemente identica ma che riporta appunti tratti dal proprio "bigino". Di sicuro è molto più brillante che nascondere un pezzettino di carta dentro la penna.

<<http://www.youtube.com/watch?v=NpQZDJ2fGnI>>

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

"Dove dovrebbe iniziare la sicurezza negli aeroporti?"

In un articolo sul blog del New York Times, Clark Ervin sostiene che la sicurezza negli aeroporti dovrebbe cominciare dalla porta principale dell'aeroporto stesso: "Come molte altre persone, passo molto tempo nei terminal degli aeroporti e spesso penso che debbano essere un bersaglio davvero appetibile per dei terroristi. Gli aeroporti più grandi sono dotati di enormi terminal che pullulano di migliaia di passeggeri ogni giorno. Sono inoltre dei simboli evidenti del consumismo americano, con i loro ristoranti McDonald's, i caffè Starbucks e i negozi di giocattoli Disney. Gli screener aeroportuali svolgono un lavoro mediocre nel controllare la presenza di pistole, coltelli e bombe ai checkpoint di sicurezza, e non esiste alcun controllo prima dei checkpoint. Pertanto, se l'obiettivo non è sferrare un attacco una volta a bordo di un aereo, ma agire all'interno dell'aeroporto stesso uccidendo le persone al suo interno, non vi è nulla che impedisca a un terrorista di farlo".

E: "Per prevenire attacchi più ridotti (e altri più estesi che potrebbero rivelarsi catastrofici), perché non spostiamo i checkpoint di sicurezza dall'interno degli aeroporti all'ingresso? Prima controlliamo i visitatori, i passeggeri e il loro bagaglio (sia fatturato che a mano) alla ricerca di eventuali pistole, coltelli ed esplosivi, prima saremo in grado di intercettare tali armi e impedire che vengano usate per distruggere e uccidere".

Sono argomentazioni ridicole, che qualsiasi lettore di questa newsletter potrebbe confutare. Se preoccupano le esplosioni a terra, qualsiasi punto in cui si dispongano i checkpoint di sicurezza sarà del tutto arbitrario. Lo scopo della sicurezza negli aeroporti è impedire atti di terrorismo SUGLI AEREI, poiché il terrorismo aereo è un problema molto più grave dei classici ordigni esplosivi fatti saltare in luoghi affollati. (Quattro

sono i motivi. Primo, le linee aeree sono spesso simboli nazionali. Secondo, gli aerei spesso volano verso paesi pericolosi. Terzo, qualsiasi siano le ragioni, pare che gli aerei sono un bersaglio preferito dai terroristi. E quarto, la caratteristica modalità di errore degli aerei fa in modo che anche una bomba di minore entità possa uccidere tutte le persone a bordo. Lo stesso ordigno fatto saltare in un aeroporto provoca la morte di poche persone e il ferimento di molte altre). E la maggior parte delle misure di sicurezza degli aeroporti sono inefficaci.

Il pregiudizio di Ervin si rivela da solo in questo passaggio: "Come molte altre persone, passo molto tempo nei terminal degli aeroporti e spesso penso che debbano essere un bersaglio davvero appetibile per dei terroristi".

Se passasse molto tempo nei centri commerciali, probabilmente penserebbe che anch'essi potrebbero essere un bersaglio davvero appetibile per dei terroristi. Anche i centri commerciali sono "simboli evidenti del consumismo americano, con i loro ristoranti McDonald's, i caffè Starbucks e i negozi di giocattoli Disney". A me sembra che Ervin sia semplicemente spaventato.

Diciamo la verità, esistono fin troppi bersagli. Occorre smetterla di difendersi contro le tattiche, per cercare invece di difendersi contro il terrorismo. La sicurezza negli aeroporti è l'ultima linea di difesa, e non è granché buona. La sicurezza, quella vera, comincia molto prima che la gente arrivi a un aeroporto, a un centro commerciale o a qualsiasi altro posto.

<<http://jetlagged.blogs.nytimes.com/2007/12/17/where-should-airport-security-begin/>>

oppure <<http://tinyurl.com/2s5zc2>>

<<http://www.schneier.com/essay-096.html>>

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

<<http://www.schneier.com/essay-121.html>>

<<http://www.schneier.com/essay-038.html>>

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

Uno studio sulla sicurezza aeroportuale

Non sorprendendo nessuno, un nuovo studio ha concluso che la sicurezza aeroportuale è inefficiente. "Un gruppo di ricercatori alla Harvard School of Public Health non ha potuto trovare un solo studio che dimostri come la lunga procedura di analisi ai raggi X del bagaglio a mano serva o sia servita a prevenire dirottamenti o attacchi. Non hanno nemmeno trovato alcuna prova che dimostri che il far togliere le scarpe ai passeggeri o la confisca di piccoli oggetti personali abbia evitato un qualche incidente".

E: "I ricercatori hanno detto che sarebbe interessante applicare standard sanitari alla sicurezza negli aeroporti. Programmi di screening per malattie come il cancro solitamente non vengono istituiti su larga scala prima di aver dato prova di funzionare".

Si noti la difesa della TSA: "Pur senza alcuna prova dell'accuratezza dei test, la Transportation Security Administration ha difeso le proprie misure di sicurezza

riportando di aver intercettato in un anno più di 13 milioni di oggetti vietati', hanno aggiunto i ricercatori. 'Molti di questi oggetti illegali erano accendini'".

Questo è il punto su cui la TSA non ha capito nulla. L'obiettivo non è confiscare oggetti vietati. L'obiettivo è di prevenire il terrorismo sugli aerei. La TSA che sequestra milioni di accendini di persone innocenti rappresenta un fallimento della sicurezza. La TSA sta reagendo a minacce inesistenti. La TSA sta reagendo a falsi allarmi. Ora, si può obiettare che questo genere di sbagli sono necessari per rendere le persone più sicure, ma di sicuro non dimostrano che le persone SONO DAVVERO più sicure.

Per esempio, non pensate che la vigilanza della TSA in fatto di torte non sia altro che uno scherzo? Sono troppo pericolose per essere introdotte sugli aerei, ma sicure quanto basta per poterle dare da mangiare ai soldati americani.

<<http://www.abcnews.go.com/Business/Travel/story?id=4034950&page=1>>

<<http://www.sciencedaily.com/releases/2007/12/071220195648.htm>>

<<http://www.alertnet.org/thenews/newsdesk/N20228618.htm>>

Lo studio:

<<http://www.bmj.com/cgi/content/full/335/7633/1290>>

La TSA e le torte:

<<http://www.oregonlive.com/oregonian/stories/index.ssf?/base/travel/1197584821232640.xml&coll=7>>

oppure <<http://tinyurl.com/yod3qq>>

La mia intervista con Kip Hawley, direttore della TSA:

<<http://www.schneier.com/interview-hawley.html>>

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

Le news su Schneier/BT Counterpane

Schneier terrà il keynote di apertura alla conferenza Technology in Wartime a Palo Alto, California, il 26 gennaio:

<<http://technologyinwartime.org/>>

Schneier intervorrà a Linux Australia a Melbourne il 30 gennaio:

<<http://linux.conf.au/>>

Schneier è stato intervistato al Computerworld Australia:

<<http://www.computerworld.com.au/index.php/id;1891124482>>

"Holy Schneier" ora è un'esclamazione:

<<http://www.schlockmercenary.com/d/20071220.html>>

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

La mia rete wireless aperta

Ogni volta che parlo o scrivo in merito alle mie impostazioni personali di sicurezza, l'unica cosa che sorprende il pubblico, e che è fonte di frequenti critiche, è il fatto che a casa mia la rete wireless sia aperta. Non c'è password. Non c'è crittografia. Chiunque dotato di collegamento wireless in grado di captare la mia rete può servirsene per navigare in Internet.

Per me è semplicemente pura cortesia. Offrire l'accesso a Internet agli ospiti è come fornire calore ed elettricità, o una bella tazza di tè caldo. Ma per certi osservatori è una cosa sbagliata e pericolosa.

Mi si dice che degli sconosciuti potrebbero starsene seduti in macchina davanti a casa mia e sfruttare la mia rete per inviare spam, intercettare le mie password, caricare e scaricare ogni genere di porcherie, da film piratati a materiale pedopornografico. Di conseguenza io correrei tutta una serie di gravissimi rischi, dal mio IP che finisce in blacklist alla polizia che fa irruzione in casa mia.

Se da un lato tutto questo è tecnicamente vero, non credo rappresenti tutto questo rischio. Ho contato almeno cinque reti wireless aperte nei caffè che si trovano nel raggio di un miglio da casa mia, ed è più probabile che un potenziale spammer si sieda in un locale climatizzato con una tazza di caffè e una fetta di torta che non in un'automobile al freddo fuori da casa mia. E sì, se qualcuno commettesse davvero un reato utilizzando la mia rete wireless potrei ricevere una visita della polizia, ma quale miglior difesa se non quella di dichiarare che possiedo una rete wireless aperta? Se attivassi la sicurezza wireless sulla mia rete e qualcuno la compromettesse con un hack, sarebbe per me molto più difficile provare la mia innocenza.

Con questo non intendo dire che WPA, il nuovo protocollo di sicurezza wireless, non sia efficace. Anzi, è molto robusto. Ma è destinato ad avere delle falle di sicurezza; ne esistono sempre alcune.

Ho parlato di tutto ciò con diversi avvocati, e tutti, con il loro tipico "legalese", hanno illustrato una serie di rischi ulteriori nel lasciare aperta la propria rete.

Se da un lato nessuno di loro ritiene che possiate essere processati e condannati solo perché qualcun altro si è servito della vostra rete, dall'altro un'indagine approfondita potrebbe andare avanti per molto tempo e risultare costosa. Il vostro computer potrebbe essere sequestrato, e se contiene del software o del materiale illecito, la situazione potrebbe diventare alquanto delicata. Inoltre i pubblici ministeri non sono proprio le persone più esperte dal punto di vista informatico, e potreste ritrovarvi dalla parte del torto malgrado la vostra innocenza. I legali con cui ho parlato hanno detto che la maggior parte degli avvocati difensori suggerirà di arrivare a un accordo invece di rischiare di essere processati con l'accusa di pedopornografia.

Parlando di una situazione meno estrema, è noto che la Recording Industry Association of America (RIAA) denuncia chi ha violato un copyright basandosi soltanto su un indirizzo IP. Le probabilità di vittoria dell'accusato sono maggiori che in un caso penale, perché nelle controversie civili l'onere della prova è minore. E anche in questo frangente gli avvocati sostengono che in caso di vittoria non vale la pena rischiare le spese, e consigliano di raggiungere un accordo e pagare qualche migliaio di dollari.

Questi scenari minacciosi, tuttavia, continuano a non convincermi del tutto. La RIAA ha portato avanti circa 26.000 cause legali, e ci sono più di 15 milioni di persone che scaricano musica. Mark Mulligan di Jupiter Research si è espresso meglio di tutti: "Se siete uno che condivide file, sapete che le probabilità di essere scoperti sono paragonabili a quelle di essere colpito da un asteroide".

Non mi smuovono nemmeno coloro che sostengono che lasciando la mia rete aperta io sto mettendo a rischio i miei dati perché degli hacker potrebbero parcheggiare davanti a casa, entrare nella mia rete e intercettarne il traffico Internet o penetrare nei miei computer. È vero, teoricamente può accadere, ma i miei computer sono più a rischio quando li collego a reti aperte negli aeroporti, nei caffè e in altri luoghi pubblici. Se configuro il mio computer in modo che sia protetto a prescindere dalla rete a cui è connesso, allora tutto il resto non ha importanza. E se il mio computer non è sicuro in una rete pubblica, allora mettere un lucchetto alla mia rete domestica non servirà molto a ridurre i rischi.

Certo, la sicurezza informatica è difficile. Ma se i computer escono da casa vostra, è un problema che va risolto comunque. E qualsiasi soluzione sarà applicabile anche alle vostre macchine desktop.

Infine i critici affermano che qualcuno potrebbe approfittare della mia rete per sottrarmi banda. Alcune isolate ordinanze giudiziarie hanno stabilito che ciò è illegale; io dico, se qualcuno vuole un po' di banda si accomodi pure. Non mi importa se i vicini di casa sfruttano la mia rete wireless quando ne hanno bisogno, e ho sentito varie storie di persone che hanno potuto far fronte a emergenze appoggiandosi a reti wireless aperte nelle vicinanze.

Allo stesso modo, mi fa piacere incontrare una rete aperta quando mi serve un collegamento. Se qualcuno stesse utilizzando la mia rete al punto di influire sulla mia navigazione o se il figlio di un vicino si mettesse a smanettarci, allora potrei prendere qualche provvedimento; ma se tutti ci comportiamo correttamente e con educazione, perché dovrei preoccuparmi? È farsi un favore reciprocamente, dico io.

Senza dubbio tutto ciò è fonte di preoccupazione per i provider Internet. Tenere una rete aperta spesso è una violazione dei termini del servizio, ma a parte l'occasionale lettera di ingiunzione o le proteste dei provider perché si è superato un limite di banda che solo loro conoscono, neanche questo rappresenta un grosso rischio. La cosa peggiore che può capitare è doversi cercare un altro provider Internet.

Una compagnia chiamata Fon ha affrontato la questione in maniera interessante. Gli access point wireless di Fon hanno due reti wireless: una sicura per il singolo utente e una aperta per tutti gli altri. È possibile configurare la propria rete sia in modalità "Bill" che in modalità "Linus". Nel primo caso la gente vi paga per poter usare la vostra rete, e voi dovrete pagare per utilizzare una qualsiasi altra rete wireless Fon. In modalità "Linus" chiunque può servirsi della vostra rete e voi potrete servirvi gratuitamente delle reti wireless Fon. È un'idea davvero brillante.

La sicurezza è sempre un compromesso. Conosco persone che chiudono a chiave la loro porta d'ingresso molto raramente, che parlano al cellulare mentre guidano sotto la pioggia, e che parlano agli sconosciuti. A mio parere non vale la pena mettere un lucchetto alla mia rete wireless. E apprezzo tutti coloro che analogamente tengono aperta la propria rete, compresi tutti i caffè, i bar e le biblioteche che ho visitato in

passato, il Dayton International Airport dove ho iniziato a scrivere questo pezzo, e il Four Points Sheraton dove l'ho concluso. Tutti voi contribuite a fare del mondo un luogo migliore.

I dati della RIAA:

<[http://www.sptimes.com/2007/10/02/Business/Minn\\_woman\\_takes\\_on\\_r.shtml](http://www.sptimes.com/2007/10/02/Business/Minn_woman_takes_on_r.shtml)>

<[http://www.npd.com/press/releases/press\\_0703141.html](http://www.npd.com/press/releases/press_0703141.html)>

<<http://www.guardian.co.uk/technology/2007/mar/22/musicnews.newmedia>>

Ordinanze sul "sottrarre banda":

<[http://www.ibls.com/internet\\_law\\_news\\_portal\\_view\\_prn.aspx?s=latestnews&id=1686](http://www.ibls.com/internet_law_news_portal_view_prn.aspx?s=latestnews&id=1686)>

oppure <<http://tinyurl.com/35wwl6>>

<<http://arstechnica.com/news.ars/post/20080103-the-ethics-of-stealing-a-wifi-connection.html>>

oppure <<http://tinyurl.com/yseb8v>>

La storia divertente di un tizio che si è messo a giocare con un "ladro di banda":

<<http://www.ex-parrot.com/~pete/upside-down-ternet.html>>

I provider Internet:

<[http://w2.eff.org/Infrastructure/Wireless\\_cellular\\_radio/wireless\\_friendly\\_isp\\_list.html](http://w2.eff.org/Infrastructure/Wireless_cellular_radio/wireless_friendly_isp_list.html)>

oppure <<http://tinyurl.com/2l6pmn>>

<[http://www.nytimes.com/2007/04/14/technology/14online.html?\\_r=1&ex=1181188800&en=06978ee1a8aa9cde&ei=5070&oref=slogin](http://www.nytimes.com/2007/04/14/technology/14online.html?_r=1&ex=1181188800&en=06978ee1a8aa9cde&ei=5070&oref=slogin)>

oppure <<http://tinyurl.com/2t5cjw>>

Fon:

<<http://www.iht.com/articles/2006/01/30/business/wireless31.php>>

<<http://www.fon.com/en/>>

Questo articolo è originariamente apparso su Wired.com.

<[http://www.wired.com/politics/security/commentary/securitymatters/2008/01/securitymatters\\_0110](http://www.wired.com/politics/security/commentary/securitymatters/2008/01/securitymatters_0110)>

oppure <<http://tinyurl.com/22s3wx>>

...E ha generato molte discussioni.

<<http://hardware.slashdot.org/article.pl?sid=08/01/10/1449228>>

Articoli contrari:

<<http://wifinetnews.com/archives/008126.html>>

<<http://www.dslreports.com/shownews/Bruce-Schneier-Wants-You-To-Steal-His-WiFi-90869>>

oppure <<http://tinyurl.com/2nqg4s>>

<<http://www.networkworld.com/community/node/23714>>

Articoli a favore:

<<http://www.boingboing.net/2008/01/10/why-its-good-to-leav.html>>

<<http://techdirt.com/articles/20080110/100007.shtml>>

<[http://blogs.computerworld.com/open\\_wireless\\_oh\\_my](http://blogs.computerworld.com/open_wireless_oh_my)>

Presumibilmente vi sarà un gran botta-e-risposta anche nei commenti sul blog.  
<[http://www.schneier.com/blog/archives/2008/01/my\\_open\\_wireles.html#comments](http://www.schneier.com/blog/archives/2008/01/my_open_wireles.html#comments)>

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

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](mailto:crypto-gram@communicationvalley.it)>

I commenti a CRYPTO-GRAM devono essere inviati a [schneier@counterpane.com](mailto: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 BT Counterpane e membro del comitato consultivo dell'Electronic Privacy Information Center (EPIC). Frequentemente scrive e partecipa a conferenze sulla sicurezza informatica e sulla 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) 2008 - Bruce Schneier.