

CRYPTO-GRAM
15 ottobre 2005

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

Edizione italiana curata da Communication Valley SpA

E-mail: schneier@counterpane.com

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

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

Crypto-Gram in versione originale è anche consultabile in formato RSS:
<http://www.schneier.com/crypto-gram-rss.xml>

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

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

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

In questo numero:

Il phishing

Grande sicurezza per un piccolo traghetto

Respinti casi di guida in stato di ebbrezza

Le ristampe di Crypto-Gram

Scanner automatici di targhe automobilistiche

La vigilanza della NSA

Leggi antiterrorismo usate per soffocare il dibattito politico

News

Deviare le rotte aeree nei pressi delle centrali nucleari

Il rapporto del Gruppo di Lavoro di Secure Flight

Il Canile: CryptIt

Le News di Counterpane

La sicurezza per gli uragani e la sicurezza aerea si scontrano

Agevolazioni fiscali per premiare una buona sicurezza

Falsificazione di certificati cartacei di basso valore

Il giudice Roberts, la privacy e il futuro

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

Il phishing

All'inizio del mese, lo stato della California è stato il primo a emettere una legge che si occupa specificamente del problema del phishing. Il phishing, per chi fosse rimasto lontano da Internet questi ultimi anni, è l'invio di un'e-mail da parte di un aggressore che si fa passare per un'azienda rispettabile e legittima allo scopo di estorcervi informazioni sensibili: le password di un vostro conto, molto spesso. Quando ciò viene fatto effettuando un hacking del DNS, si chiama pharming.

Le compagnie finanziarie finora hanno evitato di affrontare il problema in maniera seria, perché è più semplice ed economico pagare i costi delle frodi. Tuttavia è una cosa inaccettabile, perché i consumatori

vittime di queste truffe finiscono col pagare un prezzo che va al di là di una perdita economica e che si traduce in seccature, stress e, in alcuni casi, macchie sui loro conti che non è facile cancellare. Di conseguenza, i legislatori devono fare di più che non semplicemente creare nuove sanzioni per i malfattori: devono creare nuovi severi incentivi che obblighino efficacemente le compagnie finanziarie a cambiare lo status quo e a migliorare il modo con cui proteggono le risorse dei loro clienti. Purtroppo la legge californiana non fa nulla in questo senso.

La nuova legislazione è stata emanata perché il phishing è un reato nuovo, ma la legge non sarà di molto aiuto, perché il phishing è solo una tattica. I criminali usano il phishing per ottenere le vostre password, così da poter effettuare transazioni fraudolente in vostro nome. Il vero crimine è in realtà molto più antico: la frode finanziaria.

Questi attacchi sfruttano la credulità delle persone. Ciò li distingue da worm e virus, che sfruttano vulnerabilità nel codice dei computer. In passato ho definito questo genere di attacchi come esempio di "attacchi semantici" poiché fanno leva sul pensiero umano e non sulla logica di una macchina. Le vittime sono persone che ricevono e-mail e visitano siti web, e in genere credono che queste email e questi siti siano legittimi.

Questi attacchi sfruttano l'intrinseca non verificabilità di Internet. È semplice fare phishing o pharming perché autenticare un'attività in Internet è difficile. Se per un criminale potrebbe essere persino fattibile costruire una banca vera e propria per estorcere ai clienti le loro firme e i loro dettagli bancari, è assai più facile per lo stesso criminale costruire un finto sito web o inviare un'email fasulla. Se anche fosse possibile realizzare un'infrastruttura per verificare sia il sito che l'e-mail, il costo e l'entità poco user-friendly dell'operazione la renderebbero una soluzione limitata agli utenti più "geek".

Tali attacchi, poi, fanno leva sull'intrinseca scalabilità dei sistemi informatici. Per truffare qualcuno in persona occorre un certo lavoro. Attraverso l'e-mail si può provare a frodare milioni di persone all'ora. Un tasso di successo di uno su un milione potrebbe essere sufficiente a garantire un'impresa criminosa fattibile.

In generale, due tendenze in Internet influenzano ogni forma di furto d'identità. La maggiore e diffusa disponibilità di informazioni personali ha fatto in modo che un ladro possa impadronirsene con più facilità. Allo stesso tempo, la sempre maggiore diffusione dell'autenticazione elettronica e delle transazioni online (adesso non è più necessario entrare in una banca o addirittura usare un bancomat per prelevare denaro) ha reso quelle informazioni personali ancora più preziose.

Il problema del phishing non si può risolvere solamente concentrandosi sulla prima tendenza, cioè la disponibilità delle informazioni personali. I criminali sono persone intelligenti, e se ci si difende contro una tattica specifica come il phishing, loro ne troveranno un'altra. Nell'arco di pochissimi anni abbiamo visto gli attacchi di phishing divenire sempre più sofisticati. La variante più recente, detta "spear phishing" è fatta di messaggi email individualmente mirati e personalizzati, che sono ancora più difficili da rilevare. Vi sono molti altri generi di frode elettronica che non si possono definire tecnicamente phishing.

Il vero problema da risolvere è quello delle transazioni fraudolente. Le

istituzioni finanziarie rendono troppo semplice per un criminale effettuare transazioni fraudolente, e troppo difficile per le vittime ripulire i propri nomi. Le istituzioni ricavano un mucchio di denaro poiché è facile effettuare una transazione, aprire un conto, ottenere una carta di credito, e così via. Per anni ho scritto di come le considerazioni economiche influiscano sui problemi di sicurezza. Potrebbero instaurare delle contromisure di sicurezza per evitare frodi, o per rilevarle rapidamente, e permettere alle persone di sistemare la propria situazione. Ma tutto ciò è costoso e per loro non ne vale la pena.

Non è che le istituzioni finanziarie non accusino perdite. Grazie a una cosa chiamata Regulation E, esse già pagano molti dei costi diretti del furto d'identità. Ma i costi in tempo, stress e seccature sono interamente sostenuti dalle vittime. In un caso su quattro, le vittime non hanno potuto pienamente ristabilire il proprio buon nome.

In economia questo fenomeno si chiama esternalità: è un effetto di una decisione aziendale che non viene sostenuta dalla persona o dall'azienda che prende tale decisione. Le istituzioni finanziarie non hanno incentivi per ridurre quei costi di furti d'identità perché non gravano su di esse.

Si spinga la responsabilità, tutta, per il furto d'identità sulle istituzioni finanziarie, e il phishing sparirà. Questo tipo di frode sparirà non perché le persone saranno diventate più furbe e smetteranno di rispondere alle email di phishing, o perché la California vanta nuove sanzioni penali per il phishing, o perché gli ISP riconosceranno ed elimineranno le email. Sparirà perché le informazioni che un criminale potrà ottenere da un attacco di phishing non saranno sufficienti per commettere una frode. Perché le compagnie non sosterranno tutte quelle perdite.

Se esiste un precetto generale universalmente vero per una linea di condotta di sicurezza, è quello per cui la sicurezza funziona al meglio quando l'entità che si trova nella migliore posizione per mitigare i rischi è resa responsabile per tali rischi. Rendere le istituzioni finanziarie responsabili delle perdite dovute al phishing e al furto d'identità è l'unico modo di affrontare il problema. Non solo le perdite finanziarie dirette: le compagnie devono rendere meno gravosa la risoluzione delle problematiche legate al furto d'identità, permettendo alle persone di ristabilire il proprio buon nome e di ripulire il proprio profilo creditizio. Il denaro per rimborsare le perdite non è nulla in confronto alle spese per rivedere i loro sistemi, ma qualsiasi altra soluzione meno drastica non funzionerà.

La legge californiana:

[<http://www.msnbc.msn.com/id/9547692/>](http://www.msnbc.msn.com/id/9547692/)

Definizioni:

[<http://en.wikipedia.org/wiki/Phishing>](http://en.wikipedia.org/wiki/Phishing)

[<http://en.wikipedia.org/wiki/Pharming>](http://en.wikipedia.org/wiki/Pharming)

[<http://www-03.ibm.com/industries/financialservices/doc/content/news/magazine/1348544103.html>](http://www-03.ibm.com/industries/financialservices/doc/content/news/magazine/1348544103.html) oppure [<http://tinyurl.com/b32dh>](http://tinyurl.com/b32dh)

[<http://www-03.ibm.com/industries/financialservices/doc/content/news/pressrelease/1368585103.html>](http://www-03.ibm.com/industries/financialservices/doc/content/news/pressrelease/1368585103.html) oppure [<http://tinyurl.com/9rkas>](http://tinyurl.com/9rkas)

Chi paga per il furto d'identità:

[<http://www.informationweek.com/showArticle.jhtml?articleID=166402700>](http://www.informationweek.com/showArticle.jhtml?articleID=166402700)

Il mio intervento sugli attacchi semantici:

[<http://www.schneier.com/crypto-gram-0010.html#1>](http://www.schneier.com/crypto-gram-0010.html#1)

Il mio intervento su economia e sicurezza:
<<http://www.schneier.com/book-sandl-intro2.html>>

Il mio intervento sul furto d'identità:
<http://www.schneier.com/blog/archives/2005/04/mitigating_iden.html>

Dibattito sul mio articolo:
<<http://it.slashdot.org/article.pl?sid=05/10/06/199257&tid=172&tid=98>>

Questo articolo è apparso originariamente su Wired:
<<http://www.wired.com/news/politics/0,1283,69076,00.html>>

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

Grande sicurezza per un piccolo traghetto

Un traghetto che trasporta 3.000 automobili ogni giorno (in alta stagione) può essere un rischio per la sicurezza nazionale?

Può darsi, ma vale la pena istituire misure di sicurezza aggiuntive? Quanti traghetti vi sono come questo negli Stati Uniti? Quanti altri bersagli potenziali della medesima entità vi sono negli Stati Uniti? Quanto costerebbe proteggerli tutti?

Questa, semplicemente, non è la maniera di affrontare il problema.

<<http://www.virginiadot.org/infoservice/news/newsrelease.asp?ID=HRO-04-24>> oppure <<http://tinyurl.com/9kak3>>

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

Respinti casi di guida in stato di ebbrezza

Secondo l'articolo, "Centinaia di casi riguardanti test di analisi di tasso alcolico mediante respirazione sono stati respinti dai giudici di Seminole County negli ultimi cinque mesi perché il costruttore delle macchine analizzatrici non intende rivelarne il funzionamento".

Questa è la giusta decisione. Nella storia, il governo ha sempre dovuto scegliere: perseguire, o mantenere segreti i propri metodi investigativi. Non è possibile avere entrambe le cose. Se intendeva mantenere segreti i propri metodi, doveva rinunciare a perseguire.

Le persone hanno il diritto di affrontare chi le accusa. Hanno il diritto di esaminare le prove contro di loro e di contestare la validità di tali prove. Sempre più spesso le prove vengono raccolte da software: ciò si deve tradurre in attrezzature open source.

Siamo tutti più sicuri grazie a questa decisione (le cui implicazioni sono enormi: si pensi ai sistemi per il voto, per esempio).

<<http://tampatrib.com/floridametronews/MGBUBJ5QK9E.html>>

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

Le ristampe di Crypto-Gram

Crypto-Gram è attualmente al suo ottavo 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.html>. Quella che segue è una selezione di articoli apparsi in questo mese gli anni scorsi.

Mantenere segrete le interruzioni di un servizio:

<http://www.schneier.com/crypto-gram-0410.html#2>
<http://www.cryptogram.it/cryptogramPdf/Ottobre2004.pdf> (traduzione)

I passaporti RFID:

<http://www.schneier.com/crypto-gram-0410.html#3>
<http://www.cryptogram.it/cryptogramPdf/Ottobre2004.pdf> (traduzione)

L'eredità del DES:

<http://www.schneier.com/crypto-gram-0410.html#8>
<http://www.cryptogram.it/cryptogramPdf/Ottobre2004.pdf> (traduzione)

La sorveglianza all'ingrosso:

<http://www.schneier.com/crypto-gram-0410.html#10>
<http://www.schneier.com/crypto-gram-0410.html#11>
<http://www.cryptogram.it/cryptogramPdf/Ottobre2004.pdf> (traduzione)

La libertà accademica e la sicurezza:

<http://www.schneier.com/crypto-gram-0410.html#13>
<http://www.cryptogram.it/cryptogramPdf/Ottobre2004.pdf> (traduzione)

Il futuro della sorveglianza:

<http://www.schneier.com/crypto-gram-0310.html#1>
<http://www.cryptogram.it/ottobre03.htm#a1> (traduzione)

La strategia nazionale per rendere sicuro il Cyberspazio:

<http://www.schneier.com/crypto-gram-0210.html#1>
<http://www.cryptogram.it/ottobre02.htm#a1> (traduzione)

Cyber-terrorismo:

<http://www.schneier.com/crypto-gram-0110.html#1>
<http://www.cryptogram.it/ottobre.html#a1> (traduzione)

I pericoli della porta 80:

<http://www.schneier.com/crypto-gram-0110.html#9>
<http://www.cryptogram.it/ottobre.html#a9> (traduzione)

Attacchi semantici:

<http://www.schneier.com/crypto-gram-0010.html#1>

La NSA sulla sicurezza:

<http://www.schneier.com/crypto-gram-0010.html#7>

"Così vorresti diventare un crittografo":

<http://www.schneier.com/crypto-gram-9910.html#SoYouWanttobeacryptographer> oppure <http://tinyurl.com/8tk8t>

Lunghezza delle chiavi e sicurezza:

<http://www.schneier.com/crypto-gram-9910.html#KeyLengthandSecurity>

Steganografia: verità e fantasie:

<http://www.schneier.com/crypto-gram-9810.html#steganography>

Appunti per gli apprendisti scrittori di cifrati:

<http://www.schneier.com/crypto-gram-9810.html#cipherdesign>

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

Scanner automatici di targhe automobilistiche

Il Dipartimento dei Trasporti di Boston, fra i suoi doveri, emette multe per parcheggio in divieto di sosta. Se un'auto accumula troppe multe non pagate, il Dipartimento dei Trasporti aggancerà una "ganascia" a una delle ruote, rendendo il veicolo irremovibile. Dopo il pagamento di tutte le multe, il Dipartimento toglierà la ganascia.

La SUV bianca nella foto (il link è più sotto) è di proprietà del Dipartimento dei Trasporti di Boston. Il suo compito è localizzare automobili a cui deve essere applicato il fermo metallico. Le videocamere sulla sommità del veicolo sono collegate a un computer portatile su cui gira un software per scansionare le targhe automobilistiche e confrontarle con il database delle multe per divieto di sosta ancora non pagate. Quando viene trovata un'occorrenza, gli agenti del Dipartimento dei Trasporti scendono dalla macchina e applicano il fermo all'auto incriminata. Nella foto si riesce a intravedere il fermo agganciato alla ruota anteriore destra dell'auto dietro la SUV.

Questo è il genere di cose che io definisco "sorveglianza all'ingrosso", e sono già intervenuto in merito agli scanner di targhe automobilistiche in tal senso lo scorso anno.

Richard M. Smith, che ha scattato la foto, la scorsa estate ha richiesto pubblicamente al Dipartimento dei Trasporti di Boston il database dei numeri di targa scansionati e raccolti da questo veicolo. Il Dipartimento in quell'occasione ha risposto che il database non è un registro pubblico, perché il database è di proprietà di AutoVu, l'azienda canadese che realizza il software di scansione delle targhe utilizzato dal veicolo. Tale software è "concesso" alla Città di Boston come parte di un programma di prova in fase "beta".

Qualcuno ha dubbi sul fatto che AutoVu venderà questi dati a un'azienda come ChoicePoint?

AutoVu:

<http://www.autovu.com>

Il Boston Globe ha scritto in merito a questo programma:

http://www.autovu.com/website/content/pressreleases/Boston_Globe.html

La foto che ritrae la SUV bianca:

<http://www.computerbytesman.com/privacy/spycamsonwheels.jpg>

Il mio intervento sulla sorveglianza all'ingrosso:

<http://www.schneier.com/essay-057.html>

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

La vigilanza della NSA

Brevetto USA num. 6.947.978: "Metodo per localizzare geograficamente indirizzi logici di rete".

<http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=/netahtml/search-bool.html&r=1&f=G&l=50&col=AND&d=ptxt&s1=6,947,978.WKU>

.&OS=PN/6,947,978&RS=PN/6,947,978> oppure <http://tinyurl.com/8ezcq>

NSA Suite B Cryptography: scheda informativa
http://www.nsa.gov/ia/industry/crypto_suite_b.cfm

Crittografia a curva ellittica [The Case for Elliptic Curve
Cryptography]:
http://www.nsa.gov/ia/industry/crypto_elliptic_curve.cfm

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

Leggi antiterrorismo usate per soffocare il dibattito politico

Walter Wolfgang, un 82enne veterano della politica, è stato costretto ad allontanarsi dalla consultazione del Partito Laburista britannico per aver dato del bugiardo a un relatore di nome Jack Straw (le opinioni sul fatto che Jack Straw sia o meno un bugiardo sono irrilevanti in questa sede). A Wolfgang è stato poi negato l'accesso alla consultazione sulla base di leggi antiterrorismo. Si tenga presente che, fino agli anni Ottanta, le consultazioni del Partito Laburista erano avvenimenti piuttosto accesi se confrontati con gli attuali show mediatici.

Dal London Times: "Una portavoce della polizia ha dichiarato che il signor Wolfgang non è stato arrestato ma trattenuto poiché la sua autorizzazione di sicurezza è stata cancellata da funzionari Laburisti quando è stato espulso dall'aula. La portavoce ha affermato: 'Il delegato ha chiesto all'ufficiale di polizia in base a quali poteri stesse agendo, e l'ufficiale ha risposto che stava facendo valere la sua autorità in base alla Sezione 44 del Terrorism Act per confermare le generalità del delegato'".

Da The Scotsman: "Manifestanti contro la guerra in Iraq, pensionati anti-Blair e delegati della consultazione sono stati tutti trattenuti dalla polizia sulla base di una legislazione che è stata designata per combattere fanatici violenti e dinamitardi, anche se nessuno di essi era sospettato di avere collegamenti di tipo terroristico. Nessuna delle persone trattenute in custodia sulla base delle regole della Sezione 44 del Terrorism Act del 2000 è stata arrestata e nessuno è stato condannato secondo le leggi antiterrorismo.

<http://www.timesonline.co.uk/article/0,,17129-1805945,00.html>
<http://news.scotsman.com/uk.cfm?id=2028602005>

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

News

Intercettare il testo ascoltando i suoni emessi dalla tastiera:
<http://www.freedom-to-tinker.com/?p=893>
[http://www.cs.berkeley.edu/~tygar/papers/Keyboard_Acoustic_Emanations_R
evisited/preprint.pdf](http://www.cs.berkeley.edu/~tygar/papers/Keyboard_Acoustic_Emanations_Revisited/preprint.pdf)

Uno schermo con funzioni di salvaguardia della privacy. È del 2001, ma ancora interessante:
<http://www.merl.com/projects/privatedisplay/>

Ricerca sull'analisi del rischio comportamentale:
<https://www.fastlane.nsf.gov/servlet/showaward?award=0527598>

Interessante articolo di giurisprudenza sulle fonti di informazione che facilitano il compimento di un reato:

<http://www.law.ucla.edu/volokh/facilitating.pdf>

Alan Cox sui "Prossimi 50 Anni di Sicurezza Informatica". Dice molte delle cose che ho sempre sostenuto, ma più che altro riguardano i prossimi cinque anni di sicurezza informatica. Onestamente, neanche io ho idea di che cosa accadrà nei prossimi 50 anni.

<http://www.oreillynet.com/pub/a/network/2005/09/12/alan-cox.html>

Informazioni sulle macchine per il voto elettronico Diebold da parte di un impiegato Diebold. È vero, i toni sono sensazionalistici, ma vi sono anche buone informazioni.

<http://www.bradblog.com/archives/00001838.htm>

Eccellente editoriale sulla nuova imposta di capitazione in Georgia:

<http://www.nytimes.com/2005/09/12/opinion/12mon1.html?ex=1284177600&en=351bc808088315a5&ei=5090&partner=rssuserland&emc=rss> oppure

<http://tinyurl.com/cxqr5>

E qui il commento di EPIC a riguardo:

http://www.epic.org/privacy/voting/comments_ga_hb244.pdf

L'ID risolve un problema minore, e ne accentua uno più grave.

Con l'aumento dei prezzi della benzina, sono aumentate le vendite di tappi di sicurezza per il serbatoio. Qualcuno ha avuto notizia di un aumento significativo della minaccia del travaso, oppure la gente sta avendo una reazione dettata dalla paranoia?

<http://www.phillyburbs.com/pb-dyn/news/103-09042005-536764.html>

Da Israele, una truffa davvero ben congegnata per rubare un'auto e la sua identità:

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

Le telecamere di sorveglianza riprendono un'operazione di prova fatta dai terroristi del 7 luglio a Londra:

http://news.bbc.co.uk/2/hi/uk_news/4263176.stm

<http://www.nytimes.com/2005/09/21/international/europe/21london.html>

Le telecamere di sorveglianza sono tutt'altro che inutili. Credo semplicemente che non valgano il denaro speso. Vi sono contromisure molto più efficaci in cui investire denaro.

Il Dipartimento per la Sicurezza Nazionale si sta preoccupando per una minaccia da trama cinematografica: come i terroristi possano sfruttare un uragano.

http://blogs.washingtonpost.com/earlywarning/2005/09/the_pressure_co.html oppure <http://tinyurl.com/9c9m2>

Verizon sta ora monitorando i clienti per Disney. Mi sembra proprio una pessima idea.

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

Tutti sappiamo che Google può essere utilizzato per scovare ogni tipo di dati sensibili, ma qui c'è la storia di un astronomo spagnolo che è riuscito ad accedere ai registri non pubblicati del telescopio di un astronomo suo rivale su Internet.

<http://www.newscientist.com/article.ns?id=dn8033>

In questa sconcertante vicenda, un uomo viene arrestato nella metropolitana di Londra come fosse un terrorista perché... beh, perché si stava comportando da fanatico del computer.

<http://www.guardian.co.uk/attackonlondon/story/0,16132,1575532,00.html>

oppure <http://tinyurl.com/9lnr6>

Una divertente fotografia fasulla scattata nella metropolitana di Londra.

<http://www.cl.cam.ac.uk/~cpk25/outback/tube.jpg>

<http://www.snopes.com/photos/signs/tubesign.asp>

Fallimento del sistema di chiusura, basato sul riconoscimento delle impronte, di un penitenziario:

<http://www.schneier.com/blog/archives/2005/09/fingerprint-loc.html>

Un articolo sull' "Armani degli abiti antiproiettile".

<http://www.salon.com/news/feature/2005/09/22/bulletproof/index.html>

A partire dal mese prossimo, lo US-CERT inizierà ad emettere nomi uniformi per worm, virus e altro malware. Questo è parte di un programma denominato "Common Malware Enumeration Initiative" (lett. "Iniziativa per l'enumerazione del malware corrente"), ed è una buona notizia.

<http://www.eweek.com/article2/0,1895,1862251,00.asp>

Il Ministro dell'Interno della Baviera (in Germania) ha richiesto che l'industria produca contenuti Web che filtrino le "istruzioni su come costruire una bomba". Queste pagine, sostiene il Ministro, sono "un problema di sicurezza molto pericoloso". Egli spera che filtri come quelli per il controllo di materiale vietato ai minori possano risolvere il problema. Io credo che stia cercando di risolvere il problema sbagliato.

<http://makeashorterlink.com/?N25912CFB>

Alla conferenza dei Laburisti a Brighton, nel Regno Unito, gli agenti del controllo sicurezza fanno togliere alle persone gli orologi da polso per passarli attraverso lo scanner. Il motivo? Nessuno sembra saperlo.

<http://www.guardian.co.uk/g2/story/0,3604,1578937,00.html>

Secondo me tutto è cominciato come questa storia sugli altimetri, e la vicenda è stata esagerata nel raccontarla di nuovo.

http://www.schneier.com/blog/archives/2005/01/altimeter_watch.html

La sorveglianza dei telefoni cellulari porta alla cattura di criminali, perché anche i criminali portano sempre con sé i cellulari.

http://www.sptimes.com/2005/09/17/Worldandnation/Cell_phone_trails_sna.shtml

oppure <http://tinyurl.com/bo2g9>

A me sta bene che la polizia utilizzi questo strumento, a patto che il processo di ottenimento di un mandato assicuri che tale strumento non venga abusato.

Il punto di vista di un fan sulla "sicurezza" extra alle partite di football.

<http://sports.espn.go.com/espn/page2/story?page=barone/050920&num=0>

Questo "appestamento digitale" è accaduto in un gioco online, ma è comunque affascinante.

<http://www.securityfocus.com/news/11330>

Un ingegnere ha reso pubblica una falla in un chip utilizzato sull'aeromobile Airbus A380. Il conseguente insabbiamento è tristemente prevedibile.

[http://www.latimes.com/business/la-fi-whistleblower27sep27,0,7486292.st](http://www.latimes.com/business/la-fi-whistleblower27sep27,0,7486292.story)

ory> oppure <http://tinyurl.com/779pu>

Una storia sul Principe Andrea al checkpoint dell'Aeroporto di Melbourne.

http://www.guardian.co.uk/uk_news/story/0,3604,1583427,00.html

Siamo tutti più sicuri perché tutti passano attraverso i checkpoint all'aeroporto, e non esiste una white list automatica (vale la pena discutere sulle valigie diplomatiche. Un compromesso interessante).

Windows OneCare è il penetrante programma di sicurezza di prossima generazione che sarà parte di Microsoft Windows. Io non so nulla a riguardo.

<http://www.bentuser.com/article.aspx?ID=312>

Le chiavi dell'auto con chip RFID possono essere usate per tracciare persone:

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

Si può usare la crittografia per rendere anonimi questi dispositivi, ma non sussiste una ragione economica che spinga i costruttori di automobili a mettere in opera tale sistema. Ancora una volta, le barriere economiche ostruiscono la sicurezza molto più di quelle tecniche.

Si tratta di un brillante segmento di ricerca. Pare che sia possibile effettuare il jamming dei telefoni cellulari mediante i messaggi SMS. I messaggi di testo vengono trasmessi sullo stesso canale usato per impostare chiamate vocali, per cui se si inonda la rete con un tipo di comunicazione, l'altra viene tagliata fuori. I ricercatori ritengono che inviare 165 messaggi di testo al secondo è sufficiente a mettere fuori uso tutti i cellulari a Manhattan.

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

<http://www.smsanalysis.org/smsanalysis.pdf>

<http://www.gsm-security.net/forum/post-406.html>

<http://it.slashdot.org/it/05/10/05/1839217.shtml?tid=215&tid=172>

EPIC possiede informazioni sui parchi divertimenti, specie su Disney World

<http://www.epic.org/privacy/themepark/>

Disney World scansiona la geometria della mano, non le impronte digitali.

<http://www.biometricsinfo.org/handgeometry.htm>

Una minaccia da trama cinematografica: passeggeri fatti esplodere nelle linee metropolitane di New York.

<http://www.nydailynews.com/front/story/353376p-301242c.html>

La specificità della minaccia sembra un po' ridicola. Se si proibiscono i passeggeri nelle metropolitane, e i terroristi mettono i loro ordigni in sacche da viaggio, abbiamo davvero guadagnato qualcosa? Alla fine la minaccia si è rivelata uno scherzo.

<http://www.cnn.com/2005/US/10/11/nyc.scare/index.html>

I musicisti dicono ai loro fan come battere la protezione anticopia:

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

Gli inizi di un database nazionale del DNA negli Stati Uniti:

<http://www.washingtonpost.com/wp-dyn/content/article/2005/09/23/AR2005092301665.html>

oppure <http://tinyurl.com/b6otg>

Scaltro colpo da 6 milioni di dollari nel Regno Unito. Morale della storia: la sicurezza è un problema di persone, non di tecnologia. Si noti che l'artefice del colpo ha usato il "terrorismo" come pretesto.

<http://www.timesonline.co.uk/article/0,,13509-1814531,00.html>

Vi sono due proposte di legge nel Congresso che garantirebbero al Pentagono ulteriori diritti per spiare gli americani negli Stati Uniti.

<http://www.msnbc.msn.com/id/9602401/site/newsweek>

Blizzard Software si serve di spyware per verificare la conformità all'EULA:

<http://www.rootkit.com/blog.php?newsid=358>

La risposta di Blizzard:

<<http://forums.worldofwarcraft.com/thread.aspx?fn=blizzard-archive&t=33&p=1&tmp=1#post33>> oppure <<http://tinyurl.com/ey8qd>>
<<http://forums.worldofwarcraft.com/thread.aspx?FN=wow-general&T=5269471&P=1>> oppure <<http://tinyurl.com/djmzm>>

Un buon editoriale su RFID e privacy:

<http://www.boston.com/business/globe/articles/2005/10/10/you_need_not_b_e_paranoid_to_fear_rfid> oppure <<http://tinyurl.com/cngml>>

Perché Reuters crede che una carta d'identità migliore proteggerà dai furti di identità? Il problema del furto d'identità non sta nel fatto che le carte d'identità sono falsificabili, ma nel fatto che le istituzioni finanziarie non le controllano prima di autorizzare transazioni.

<<http://today.reuters.com/news/newsArticleSearch.aspx?storyID=164326+10-Oct-2005+RTRS&srch=cheye>> oppure <<http://tinyurl.com/7f5ap>>

I progressi della tecnologia porteranno un migliore screening basato su tracce chimiche.

<<http://www.wired.com/news/privacy/0,1848,69137,00.htm>>

Mentre questo tipo di tecnologia migliora, aumentano anche i problemi legati ai falsi allarmi. Sappiamo già che un'alta percentuale di banconote statunitensi presenta tracce di cocaina, ma può un terrorista da quattro soldi far chiudere un aeroporto spruzzando tracce di sostanze chimiche a caso sui bagagli dei passeggeri mentre questi non guardano?

Checkpoint di sicurezza giocattolo di Playmobil:

<http://store.playmobilusa.com/is-bin/INTERSHOP.enfinity/eCS/Store/en/-/USD/PM_DisplayProductInformation-Start?ProductSKU=3172> oppure

<<http://tinyurl.com/cg6vt>>

<http://www.concurringopinions.com/archives/2005/10/the_airline_scr.html>

>

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

Devviare le rotte aeree nei pressi delle centrali nucleari

Il governo tedesco vuole effettuare il jamming della strumentazione di navigazione aerea nei pressi di centrali nucleari.

Questo sarebbe senza dubbio utile se i terroristi volessero dirigere un aereo contro una centrale nucleare, ma mi sa di minaccia da trama cinematografica. Inoltre, una cosa del genere potrebbe peggiorare di molto la situazione nel caso in cui un aereo vola vicino a una centrale nucleare per sbaglio. Ho la sensazione che ciò accada molto più spesso rispetto all'eventuale minaccia terroristica.

<http://www.expatica.com/source/site_article.asp?subchannel_id=26&story_id=23759> oppure <<http://tinyurl.com/dpk9b>>

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

Il rapporto del Gruppo di Lavoro di Secure Flight

Da gennaio di quest'anno sono stato un membro del Gruppo di Lavoro di Secure Flight, valutando la sicurezza e la privacy del programma. Lo scorso mese abbiamo emesso il nostro rapporto.

Onestamente, non ho preso parte alla scrittura. Durante i lavori ho lasciato perdere, stanco di non poter ottenere alcuna risposta dalla TSA, e credendo che il rapporto sarebbe finito nel cassetto della scrivania di qualcuno, per non vedere mai più la luce. Sono rimasto sbalordito quando ho saputo che l'ASAC lo ha reso pubblico.

C'è parecchia carne al fuoco nel rapporto, ma vorrei citare la sezione che illustra le domande essenziali a cui la TSA non è stata in grado di dare una risposta:

"Il Gruppo di Lavoro di Secure Flight ha riscontrato che la TSA non ha saputo dare una risposta ad alcune domande chiave su Secure Flight: in primo luogo, la TSA non ha delineato quali sarebbero gli obiettivi specifici di Secure Flight. Basandoci sui risultati incompleti dei test a noi presentati, non ci è possibile stabilire neanche se l'obiettivo generale della valutazione dei passeggeri per il rischio che rappresentano per la sicurezza aerea sia realistico o realizzabile né come la TSA intenda raggiungerlo. Non sappiamo quante né quali informazioni personali saranno raccolte dal sistema o come i dati provenienti da varie fonti confluiranno nel sistema.

"Finché la TSA non risponderà a queste domande, è impossibile valutare il potenziale impatto del programma sulla privacy o sulla sicurezza, includendo problematiche quali:

- * Minimizzare i falsi positivi e gestirli quando avvengono.
- * Uso scorretto delle informazioni presenti nel sistema.
- * Accesso inopportuno o illegale da parte di persone con o senza autorizzazione.
- * Come evitare l'utilizzo del sistema e delle informazioni elaborate attraverso il sistema per scopi diversi dallo screening dei passeggeri delle linee aeree.

"Le seguenti domande ampiamente definite rappresentano le problematiche fondamentali che crediamo la TSA debba affrontare prima che noi o un qualsiasi altro organo consultivo possa stabilire effettivamente l'impatto sulla privacy e sulla sicurezza di Secure Flight sul pubblico.

"*Qual è l'obiettivo, o gli obiettivi, di Secure Flight? La TSA è sotto mandato governativo e ha ordine di confrontare elenchi di passeggeri delle linee aeree statunitensi con una consolidata watch list di terroristi. La TSA non è stata in grado di specificare con coerenza se questo confronto di elenchi sia l'unico obiettivo di Secure Flight in questa fase. Il 'Secure Flight Capabilities and Testing Overview' [Introduzione alle possibilità e alle verifiche di Secure Flight] un documento interno consegnato al Gruppo di Lavoro e datato 9 febbraio 2005, afferma nell'Appendice che il programma non è alla ricerca di terroristi sconosciuti né ha l'intenzione di farlo. Il 29 giugno 2005, Justin Oberman (vice amministratore di Secure Flight/Registered Traveler) ha testimoniato di fronte a una commissione governativa, sostenendo che "un altro obiettivo proposto per Secure Flight è quello di impiegarlo per instaurare 'meccanismi per setacciare accuratamente informazioni su criminali violenti'". Infine, la TSA non è mai stata chiara nell'indicare se possieda uno scopo ulteriore e implicito per quanto riguarda il tracciamento di sospettati di terrorismo (la cui presenza sulla watch list di terroristi non significa necessariamente che abbiano intenzione di commettere atti di violenza durante un volo).

"Mentre il problema di non riuscire a stabilire degli obiettivi chiari per Secure Flight può sorgere a un certo punto dal non riconoscere la differenza fra definizione del programma ed evoluzione del programma, questa è chiaramente una problematica che la TSA deve affrontare se intende procedere con Secure Flight.

"Qual è l'architettura del sistema di Secure Flight? Il Gruppo di Lavoro ha ricevuto scarse informazioni in merito all'architettura tecnica di Secure Flight e nessuna informazione sulle scelte compiute in materia di hardware e software. Sappiamo molto poco di come i dati verranno raccolti, trasferiti, analizzati, registrati o cancellati. Malgrado il nostro compito sia quello di valutare la privacy e la sicurezza del sistema, non abbiamo visto alcuna dichiarazione né politiche e procedure di privacy oltre alle note del Privacy Act pubblicate nel Registro Federale per i test di Secure Flight. Non è stato inoltre fornito né discusso alcun piano di gestione dei dati né per la fase di prova né per il programma così come è implementato.

"Secure Flight sarà collegato ad altre applicazioni della TSA? Il collegamento ad altri programmi di screening (come Registered Traveler, Transportation Worker Identification and Credentialing (TWIC), e sistemi di controllo di frontiera come U.S.-VISIT) che possano operare sulla medesima piattaforma di Secure Flight è un altro aspetto della domanda sull'architettura e sicurezza. Rimangono senza risposta le domande in merito a come Secure Flight andrà a interagire con altri programmi di scrutinio operanti sulla stessa piattaforma; su come garantirà che le sue linee di condotta sulla raccolta, utilizzo e conservazione dei dati saranno implementate e fatte rispettare su una piattaforma che allo stesso tempo attua programmi con linee di condotta estremamente diverse in queste aree; e come andrà a interagire con lo scrutinio dei passeggeri di voli internazionali?

"Come saranno utilizzate le fonti di dati commerciali? Uno degli elementi in assoluto più controversi di Secure Flight è stato questo, ossia i possibili impieghi dei dati commerciali. La TSA non ha mai definito con chiarezza due problematiche d'ingresso: che cosa intenda per "dati commerciali", e come possa utilizzare le fonti di dati commerciali nell'implementazione di Secure Flight. La TSA non ha mai chiaramente fatto distinzioni fra i vari impieghi possibili dei dati commerciali, che hanno tutti svariate implicazioni.

"I possibili impieghi di dati commerciali a volte descritti dalla TSA includono: (1) verifica o autenticazione dell'identità; (2) riduzione dei falsi positivi mediante l'aumento di record dei passeggeri indicanti una possibile coincidenza con dati che possano contribuire a distinguere un passeggero innocente da qualcuno presente su una watch list; (3) riduzione dei falsi negativi mediante l'aumento di tutti i record dei passeggeri con dati che potrebbero suggerire un'occorrenza che altrimenti non sarebbe stata rilevata; (4) identificazione di "spie occulte", che a sua volta comprende: (a) identificazione di false identità; (b) rilevamento di comportamenti che indicherebbero attività terroristica. Una quinta possibilità non è stata discussa dalla TSA: l'utilizzo di dati commerciali per aumentare le voci delle watch list in modo da migliorarne l'accuratezza. Assumendo che la verifica dell'identità è parte di Secure Flight, quali sono le conseguenze se una certa identità non può essere verificata con un livello sufficiente di certezza?

"È importante notare come la TSA non abbia mai presentato al Gruppo di Lavoro i risultati dei suoi test con i dati commerciali. Finché i risultati di questi test non saranno disponibili e non saranno stati analizzati indipendentemente, i dati commerciali non devono essere utilizzati nel programma Secure Flight.

"*Quali algoritmi funzionano al meglio per effettuare i confronti? La TSA non ha mai presentato al Gruppo di Lavoro risultati di test che illustrino l'efficacia di algoritmi utilizzati per confrontare i nomi dei passeggeri con una watch list. Un obiettivo dell'impiegare il

confronto basato su watch list all'interno del governo era quello di garantire l'impiego uniforme della migliore tecnologia di confronto. Il Gruppo di Lavoro di Secure Flight non ha visto alcuna prova che la TSA abbia provato diversi prodotti e soluzioni concorrenti. La TSA non ha descritto al Gruppo di Lavoro i propri criteri per stabilire come sarebbe stata determinata la soluzione di confronto ottimale. Vi sono dei compromessi ovvi e alcuni forse meno ovvi tra falsi positivi e falsi negativi, ma la TSA non ha spiegato come conciliare queste problematiche.

"Quali sono la struttura e la linea di condotta della supervisione di Secure Flight? La TSA non ha prodotto un documento di policy esauriente per Secure Flight che definisca la supervisione o le responsabilità governative".

I membri del Gruppo di Lavoro e i firmatari del rapporto sono Martin Abrams, Linda Ackerman, James Dempsey, Edward Felten, Daniel Gallington, Lauren Gelman, Steven Lilenthal, Anna Slomovic e il sottoscritto.

Vi è un'altra piega bizzarra di questa storia. Verso la fine dei lavori, la TSA ha assunto un certo Larry Ponemon per assisterci nella scrittura del rapporto. Aveva due compiti: il primo, di correggere quel che avevamo da dire, e il secondo di spingere i membri del Gruppo di Lavoro a scrivere qualcosa di omogeneo. Ma pare che la TSA gli affidò anche un terzo compito segreto: scrivere un documento di verifica del nostro lavoro. Per cui da una parte Ponemon era il nostro segretario e project leader, dall'altra era una spia della TSA.

Trovo immorale tutto questo, anche se è chiaro che Ponemon è stato abbindolato dalla TSA (Ponemon si è difeso nei nostri confronti dicendo che non credeva che il suo rapporto sarebbe stato reso pubblico. Si è rifiutato di dichiarare alcunché in pubblico a riguardo, poiché presumo voglia lavorare ancora con la TSA in futuro).

Il suo rapporto dice sostanzialmente che la TSA sta facendo tutto per bene, ma che semplicemente la documentazione non era disponibile per il Gruppo di Lavoro quando abbiamo scritto il nostro rapporto. Questo è falso, e presumo che Justin Oberman gli abbia semplicemente mentito in modo convincente. Ma la questione è ora in mano al Data Privacy and Integrity Advisory Committee (Commissione consultiva sulla privacy e integrità dei dati) del Dipartimento per la Sicurezza Nazionale.

Il nostro rapporto:

<http://www.tsa.gov/interweb/assetlibrary/SFWG_Report_September_19_2005_Final_V_1_.4.pdf> oppure <<http://tinyurl.com/ccyzj>>
<http://www.epic.org/privacy/airtravel/sfwg_report_091905.pdf>

Il rapporto di Ponemon:

<http://www.tsa.gov/interweb/assetlibrary/Ponemon_Institute_report_Final_V_1_.4.pdf> oppure <<http://tinyurl.com/9o6g7>>

L'Ispettore Generale del Dipartimento di Giustizia degli Stati Uniti il mese scorso ha rilasciato un rapporto su Secure Flight, concludendo in sostanza che i costi erano fuori controllo e che la TSA non aveva idea di quanto sarebbe costato il programma in futuro.

<<http://www.usdoj.gov/oig/reports/FBI/a0534/final.pdf>>

Per chi crede che le cose stiano migliorando, qui c'è la storia di come la no-fly list sia costata il posto di lavoro a un pilota:

<http://www.boston.com/news/local/massachusetts/articles/2005/09/22/no_fly_action_takes_pilots_job> oppure <<http://tinyurl.com/864eu>>

EPIC ha ricevuto una serie di documenti riguardanti i continui problemi

Le News di Counterpane

Counterpane citata in un articolo di CIO Decisions magazine:
<<http://www.counterpane.com/news-cio.html>>

Schneier interverrà alla conferenza RSA Europe a Vienna il 18-19 ottobre:
<<http://2005.rsaconference.com/europe/>>

Schneier interverrà a Data Security 2005 a Helsinki il 27 ottobre:
<<http://www.tieturi.fi/koulutus/seminaarit/ds2005/etusivu.asp>>

Schneier interverrà al CSO Executive Forum a Denver il 4 novembre:
<<http://ciso.issa.org/events/forum.html>>

Schneier interverrà alla Facoltà di Giurisprudenza dell'UCLA a Los Angeles il 7 novembre:
<<http://www.lawtechjournal.com>>

** *** *****

La sicurezza per gli uragani e la sicurezza aerea si scontrano

Nei giorni precedenti l'uragano Rita, durante l'evacuazione di Houston, circa 100 agenti di sicurezza aerea non si sono presentati al lavoro (presumibilmente anch'essi avevano evacuato). Il risultato: lunghe code e voli perduti, mentre la TSA si affannava per inviare un team di agenti di sicurezza sostitutivo proveniente da Cleveland.

Questo è folle. La TSA ha il permesso di utilizzare procedure di screening "alternative" in determinate circostanze. Non è una decisione facile da prendere, ma a volte la cosa più intelligente da fare in un'emergenza è quella di sospendere le regole di sicurezza. Certo che vi sono dei rischi, ma è un compromesso sensato.

Il perché ciò non sia accaduto è un esempio di agenda e di priorità. Se da un lato è sensato lasciar salire queste persone sugli aerei, chiunque aveva l'autorizzazione per prendere una decisione del genere doveva essere preoccupato per il proprio posto di lavoro. Se fosse successo qualcosa, malgrado l'improbabilità di una tale eventualità, sarebbe stato licenziato. D'altra parte, rifiutandosi di cambiare le regole, centinaia di persone sarebbero partite con ritardo, ma la cosa non avrebbe influito sulla sua posizione.

<<http://www.kink.fm/index.php/weblog/more/115/>>

** *** *****

Agevolazioni fiscali per premiare una buona sicurezza

Il Congresso sta pensando (sta solo pensando, ma almeno l'idea c'è) di concedere agevolazioni fiscali alle aziende che dimostrano una buona sicurezza cibernetica.

Si dice che il diavolo è nei dettagli, e questo potrebbe risultare una notizia priva di senso, ma l'idea è solida. Le aziende assennate vanno a proteggere le loro risorse solo per il valore che hanno *per quella

azienda*. Il problema è che molti dei rischi di sicurezza delle risorse digitali non sono rischi per la compagnia che le possiede. Questa è un'esternalità. Per cui, se tutti abbiamo bisogno che un'azienda protegga le proprie risorse digitali a un maggior livello, allora dobbiamo pagare per quella protezione in più (almeno è ciò che facciamo in una società capitalista). Possiamo pagare attraverso la normativa o attraverso le responsabilità, che si traduce in prezzi più alti per qualsiasi attività svolga l'azienda. Possiamo pagare finanziando direttamente quella sicurezza aggiunta, staccando un assegno o riducendo le tasse. Ma non possiamo aspettarci che una compagnia investa il denaro in più come un atto spontaneo di buon cuore.

<http://news.com.com/Tax+breaks+for+cybersecurity+firms/2100-7348_3-5884149.html> oppure <<http://tinyurl.com/dr4qo>>

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

Falsificazione di certificati cartacei di basso valore

Sia Subway che Cold Stone Creamery hanno chiuso i loro programmi frequent-purchaser perché la documentazione cartacea si può falsificare troppo facilmente (l'articolo dice che timbri falsi di Subway sono in vendita su eBay).

Una volta la difficoltà di contraffare la carta era un deterrente sufficiente a garantire la sicurezza di questo genere di applicazioni a basso valore. Oggi che il desktop publishing e la stampa sono molto comuni, le cose sono cambiate. Subway sta implementando un sistema basato su carte a striscia magnetica. Qualcuno vuole provare a indovinare quanto tempo passerà prima che salti fuori un hack?

<<http://www.wired.com/news/business/0,1367,68909,00.html>>

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

Il giudice Roberts, la privacy e il futuro

Ai "confirmation hearing" di John Roberts, non vi furono abbastanza discussioni sulla fantascienza. Quelle tecnologie che sono fantascienza oggi diventeranno problematiche costituzionali prima che Roberts si ritiri. Stesso dicasi per quelle tecnologie che oggi non si possono nemmeno immaginare. E molte di queste problematiche hanno a che vedere con la privacy.

Secondo Roberts esiste un "diritto alla privacy" nella Costituzione. Almeno, questo è quanto ha dichiarato nel corso delle udienze al Senato la settimana scorsa. È una questione carica di politica, perché le due decisioni che stabilirono il diritto ai contraccettivi e all'aborto [Griswold vs. Connecticut (1965) e Roe vs. Wade (1973)] sono in parte basate su un diritto alla privacy. "Qual è la tua posizione sulla privacy?" può essere un modo di chiedere "Qual è la tua posizione sull'aborto?"

Ma le problematiche costituzionali sulla privacy presentano un ambito molto più esteso. I recenti progressi tecnologici hanno già presentato profonde implicazioni legate alla privacy, e c'è ogni ragione di credere che questa tendenza proseguirà in futuro. Roberts ha 50 anni. Se verrà confermato, potrebbe essere presidente della Corte Suprema per altri 30 anni. È un bella fetta di futuro.

Le questioni sulla privacy verranno sollevate dalle azioni del governo nella "Guerra al Terrore"; verranno sollevate dalle azioni di aziende e singoli individui. Comprenderanno problematiche di sorveglianza, di profiling, ricerca e cattura. E le decisioni della Corte Suprema su tali problematiche avranno un grandissimo effetto sulla società.

Alcuni esempi. I progressi nel tracciare la mappa genetica continuano, e un giorno tutto questo sarà semplice, economico e molto approfondito, e si potrà farlo all'insaputa del soggetto. Quali protezioni di privacy hanno le persone per la loro mappa genetica, visto che vi sono copie del loro genoma in ogni cellula epidermica morta che si lasciano dietro? Quali protezioni hanno le persone contro azioni del governo basate su questi dati? O contro azioni di privati?

Quando si concede un mutuo o si determina il tasso di interesse, si dovrebbe tenere in considerazione il patrimonio genetico del cliente?

La sorveglianza è un'altra area in cui i progressi tecnologici solleveranno nuove problematiche costituzionali. Ho già scritto a riguardo della sorveglianza all'ingrosso, la capacità del governo di raccogliere i dati di chiunque per poi esaminarli nella ricerca di specifici individui. Stiamo già vedendo in azione questo tipo di sorveglianza con gli scanner automatici di targhe automobilistiche e le fotografie aeree.

In futuro tutto questo diventerà più personale. Nuove tecnologie saranno in grado di vedere attraverso i muri, sotto i vestiti, sotto la pelle, forse addirittura di osservare l'attività cerebrale. Il Senatore Joseph Biden (D-Delaware) ha chiesto retoricamente a Roberts: "È possibile impiantare segnalatori microscopici nel corpo di una persona per tracciarne ogni momento?... È possibile utilizzare scansioni cerebrali per determinare se una persona ha la tendenza verso comportamenti violenti o criminali?" Quali dovrebbero essere i limiti su ciò che può fare la polizia senza un mandato?

Citato in un articolo del New York Times, il sostenitore della privacy Marc Rotenberg ha dipinto il seguente scenario: un giorno, in un futuro prossimo, un giovane uomo sta camminando intorno al Monumento di Washington per una mezz'ora. Le telecamere riprendono il suo viso, che rivela un'identità. Tale identità viene fatta passare in vari database commerciali, producendo lo storico dei suoi viaggi, un elenco di riviste a cui è iscritto e altri dati personali. Tutto questo viene dato in pasto a un sistema di classificazione elettronico, che lo dichiara come potenziale minaccia terroristica. Egli viene fermato dalla polizia, che apre il suo zaino e trova una busta di marijuana. L'apertura dello zaino è da considerarsi una perquisizione legale secondo quanto definito dalla Costituzione?

Questa storia illustra una serie di tecnologie che potrebbero diventare molto comuni nei prossimi anni. Il rilevamento facciale automatizzato permetterà a polizia, aziende e individui di identificare le persone a loro insaputa e senza il loro permesso. Programmi di data mining setacceranno montagne di dati, nuovi e vecchi, e selezioneranno chi deve essere sottoposto a ulteriori indagini. E le persone potrebbero venire accusate di cospirazione basandosi su niente più che una trama nebulosa di eventi.

Analogamente, è possibile che le aziende effettuino lo stesso tipo di raccolta dati e utilizzino i risultati per negare un posto di lavoro, o un'assicurazione sanitaria, o un mutuo?

Nei prossimi anni la Corte Suprema affronterà casi come questi. A

a cui recapitare la newsletter, visitate:
<<http://www.schneier.com/crypto-gram.html>>

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

La versione italiana è curata da Communication Valley SpA
<http://www.communicationvalley.it/>.

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

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

Per informazioni crypto-gram@communicationvalley.it.

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

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

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

Copyright (c) 2005 by Bruce Schneier.