

riconteggio. Il collegio elettorale sceglierà un vincitore da mandare a Washington, ma non perché si è certi che la maggioranza abbia votato per lui. Può darsi di sì, come può darsi di no. Non vi è modo di saperlo.

Le macchine per il voto elettronico rappresentano una grave minaccia per elezioni giuste e precise, una minaccia che dovrebbe preoccupare ogni cittadino americano, sia egli Repubblicano Democratico o indipendente. Dato che le elezioni sono computerizzate, sono sufficienti le azioni deliberate o accidentali di pochi per mandarle a monte. La soluzione: schede cartacee, che possono essere verificate dai votanti stessi e riconteggiate se necessario.

Per comprendere la sicurezza delle macchine per il voto elettronico, occorre prima considerare la sicurezza delle elezioni in generale. Lo scopo di ogni sistema di voto è quello di "catturare" le diverse volontà espresse da ogni votante e di raccoglierle tutte in un conteggio finale. Nella prassi, si tratta di un trasferimento che avviene mediante una serie di passaggi. Quando ho votato, la scorsa settimana, ho trasferito la mia volontà su una scheda cartacea, la quale è stata poi trasferita ad una macchina per tabulazioni attraverso uno scanner; a fine giornata i funzionari elettorali hanno passato i conteggi automatici individuali ad una struttura centralizzata che li ha combinati in un unico risultato che ho poi visto in televisione.

Tutti i problemi delle elezioni non sono altro che errori introdotti in uno qualsiasi di questi passaggi, siano essi voti nulli per privazione di diritti elettorali, schede non chiare, macchine guaste, o voti fraudolenti. Anche durante operazioni normali, ognuno di tali passaggi può introdurre degli errori. Per garantire una precisione del voto, pertanto, è necessario 1) ridurre al minimo il numero di passaggi, e 2) aumentare l'affidabilità di ogni passaggio.

Molta della nostra sicurezza elettorale è basata sulla "sicurezza per conflitto di interessi". Ogni passaggio, a eccezione della compilazione della scheda anonima da parte del votante, viene osservato da un rappresentante di ogni maggiore partito politico; ciò garantisce che qualsiasi imbroglio di parte, ma anche un eventuale errore in buona fede, non sfugga agli altri osservatori. Non è un sistema perfetto, ma funziona benissimo da un paio di secoli a questa parte.

Il voto elettronico è come un iceberg: le vere minacce si nascondono ben al di sotto del livello dell'acqua. Le macchine per il voto elettronico prive di supporto cartaceo aggirano il processo di sicurezza menzionato poco sopra, permettendo a uno sparuto gruppo di persone, o addirittura a un singolo hacker, di influenzare un'elezione. Il problema è il software, programmi che non vengono mostrati e che non possono essere verificati da un team di giudici elettorali Repubblicani e Democratici, programmi che possono modificare drasticamente i conteggi finali. E visto che tutto quel che rimane alla fine della giornata elettorale sono tali conteggi elettronici, non vi è modo di verificare i risultati o di effettuare un riconteggio. I riconteggi sono importanti.

Questa non è teoria. Negli Stati Uniti vi sono stati finora centinaia di casi documentati di macchine per il voto elettronico che hanno distorto i voti ai danni di candidati di entrambi i partiti: macchine che hanno perso voti, macchine che hanno scambiato i voti dei candidati, macchine che hanno registrato un numero maggiore di voti a favore di un candidato rispetto al numero totale degli elettori, macchine che non hanno registrato alcun voto. Mi piacerebbe credere che in tutti questi casi si è trattato di errori e non di frodi deliberatamente perpetrate, ma la verità è che non è possibile distinguere le due cose. E questi sono soltanto i problemi in cui ci si è imbattuti: quasi certamente ve ne sono stati molti altri passati inosservati perché nessuno stava

prestando attenzione.

Ciò è al tempo stesso un fenomeno nuovo e sconcertante. Nella maggior parte dei casi, nell'arco della storia, la frode elettorale su vasta scala non si è potuta attuare con facilità: occorrono azioni davvero pubbliche o un governo estremamente corrotto, o entrambe le cose. Ma il voto elettronico è diverso: un solo hacker può influenzare un'elezione. Può svolgere il suo lavoro di nascosto prima che le macchine vengano inviate ai vari seggi elettorali. Può condizionare le macchine per il voto di un'intera regione. E può cancellare completamente le proprie tracce, scrivendo codice che si autoelimina dopo le elezioni.

E tutto questo presume macchine per il voto ben progettate. Quelle vendute da compagnie come Diebold, Sequoia Voting Systems ed Election Systems & Software sono molto peggio. La qualità del software è mediocre. Le macchine sono "protette" da chiavette come quelle dei minibar negli alberghi. I conteggi dei voti vengono archiviati in file facilmente modificabili. Le macchine possono essere infettate da virus. Certo software per il voto gira sotto Microsoft Windows, con tutti i bug, i crash e le vulnerabilità che tale sistema operativo comporta. L'elenco delle pratiche di sicurezza inadeguate è lunghissimo.

Le aziende produttrici delle macchine per il voto ribattono sostenendo che tali attacchi sono impossibili da attuare poiché le macchine non vengono mai lasciate incustodite (non è vero), che le schede di memoria su cui vengono conservati i voti vengono controllate accuratamente (non è così), e che tutto viene sorvegliato (falso anche questo). Sì, mentono, ma soprattutto non stanno comprendendo il problema.

Non dovremmo, e non dobbiamo, accettare macchine per il voto che magari, un bel giorno, potranno essere sicure se e solo se viene eseguita alla lettera una lunga sequenza di procedure operative. Abbiamo bisogno invece di macchine per il voto che siano sicure a prescindere da come vengono programmate, maneggiate e utilizzate, e di cui ci si possa fidare anche se sono distribuite da un'azienda di parte, o da una società con possibili legami con il Venezuela.

Sembra un compito impossibile, ma in realtà la soluzione è sorprendentemente semplice: occorre utilizzare le macchine per il voto elettronico come generatrici di schede cartacee. Si voti con qualsivoglia interfaccia touch-screen; la macchina non registrerà né conserverà i conteggi di come le persone hanno votato: emetterà semplicemente una scheda cartacea. Il votante potrà controllarla per verificare che sia tutto a posto, poi la scheda verrà processata da una seconda macchina, uno scanner. Essa produrrà un veloce conteggio iniziale, mentre la scheda cartacea rimarrà a disposizione in caso sia necessario un riconteggio. E allo stesso modo si possono conteggiare le schede di backup e i voti di chi non ha potuto recarsi a votare e ha inviato il voto per posta.

Si potrebbe anche eliminare del tutto le macchine per la generazione del voto elettronico e segnare a mano le schede come si fa in Minnesota. O indire un'elezione totalmente basata sull'invio dei voti a mezzo posta, come avviene nell'Oregon. Ancora una volta, la chiave di tutto sono le schede cartacee.

La carta? Certo, la carta. Una pila di carta è molto più difficile da alterare che non dei numeri nella memoria di un computer. Gli elettori possono vedere il proprio voto su carta, a prescindere da quel che accade all'interno del computer. Ma soprattutto nessuno ha problemi a comprendere e maneggiare la carta. Le bollette del telefono cellulare e gli addebiti errati sulla carta di credito ci creano sempre qualche difficoltà, ma qual è stata l'ultima volta che abbiamo avuto problemi

con un biglietto da 20 dollari? Sappiamo come si conta la carta. Le banche non fanno altro che contarla. Sia il Canada che il Regno Unito contano schede elettorali cartacee senza problemi, stesso dicasi per gli svizzeri. Lo possono fare anche gli Stati Uniti. Oggi, fra i vari crash informatici, worm e hacker, una soluzione low-tech è la più sicura.

Le macchine per il voto sicure sono solamente uno dei componenti di un'elezione onesta e corretta, ma ne rappresentano una parte sempre più importante. Sono il punto in cui un aggressore scrupoloso può commettere frode elettorale nella maniera più efficace (e sappiamo tutti che cambiare i risultati di un'elezione può valere milioni di dollari). Ma non dobbiamo dimenticarci di altre tattiche di "dirottamento": indirizzare le persone al seggio sbagliato o riferire una data sbagliata per il giorno delle elezioni, eliminare votanti registrati dalle liste elettorali, sistemare un numero troppo ridotto di macchine per il voto nei seggi elettorali, o rendere oneroso il procedimento di registrazione per votare. (Per quanto possa sembrare strano, i voti di chi non ha i requisiti per votare non rappresentano un problema negli Stati Uniti, malgrado la retorica politica sostenga il contrario; tutti gli studi condotti a riguardo mostrano che il numero di tali voti è così basso da essere insignificante. E l'obbligo di presentare un documento d'identità con foto causa in realtà più problemi di quanti ne risolva.)

Il voto è una questione percettiva al pari di una problematica tecnologica. Non basta che il risultato sia matematicamente preciso: ogni cittadino deve anche fidare nella sua correttezza. Nel mondo, le persone protestano o insorgono dopo un'elezione non quando il loro candidato ha perso, ma quando ritengono che il loro candidato abbia perso ingiustamente. Per una democrazia è essenziale che un'elezione determini con accuratezza un vincitore e al tempo stesso convinca il perdente in maniera soddisfacente. Negli Stati Uniti stiamo perdendo il fattore percettivo.

L'attuale gruppo di macchine per il voto elettronico fallisce in entrambi i fronti. I risultati del 13esimo Collegio Elettorale della Florida non sono né precisi né convincenti. Come democrazia, meritiamo qualcosa di meglio. Dobbiamo rifiutarci di votare usando macchine per il voto elettronico che non producono una scheda cartacea verificabile dal votante, e dobbiamo continuare a fare pressioni sulle nostre entità legislative affinché si implementi una tecnologia di voto che funzioni realmente.

Questo articolo è originariamente apparso su Forbes.com.

http://www.forbes.com/home/security/2006/11/10/voting-fraud-security-tech-security-cz_bs_1113security.html

<http://www.schneier.com/essay-068.html>

http://www.schneier.com/blog/archives/2004/11/the_problem_wit.html

<http://www.votingintegrity.org/archive/news/e-voting.html>

<http://www.verifiedvoting.org/article.php?id=997>

<http://www.ecotalk.org/VotingMachineErrors.htm>

http://evote-mass.org/pipermail/evote-discussion_evote-mass.org/2005-January/000080.html oppure <http://tinyurl.com/yhvb2a>

<http://avirubin.com/vote/analysis/index.html>

<http://www.freedom-to-tinker.com/?p=1080>

<http://www.freedom-to-tinker.com/?p=1081>

<http://www.freedom-to-tinker.com/?p=1064>

<http://www.freedom-to-tinker.com/?p=1084>

<http://www.bbvforums.org/cgi-bin/forums/board-auth.cgi?file=/1954/15595.html> oppure <http://tinyurl.com/9ywcw>

<http://itpolicy.princeton.edu/voting>

http://www.ss.ca.gov/elections/voting_systems/security_analysis_of_the_diebold_accubasic_interpreter.pdf oppure <http://tinyurl.com/eqpbd>

<http://www.blackboxvoting.org>
http://www.brennancenter.org/dynamic/subpages/download_file_38150.pdf
<http://avirubin.com/judge2.html>
<http://avirubin.com/judge.html>
http://www.usatoday.com/news/washington/2006-10-29-voting-systems-probe_x.htm oppure <http://tinyurl.com/ylnba6>

Come vincere illegalmente le elezioni:

<http://arstechnica.com/articles/culture/evoting.ars>

Florida 13:

<http://www.heraldtribune.com/apps/pbcs.dll/article?AID=/20061111/NEWS/611110643> oppure <http://tinyurl.com/ygo73l>
<http://www.heraldtribune.com/apps/pbcs.dll/article?Date=20061108&Category=NEWS&ArtNo=611080506> oppure <http://tinyurl.com/yahvve>
<http://www.heraldtribune.com/apps/pbcs.dll/article?AID=/20061109/NEWS/611090343> oppure <http://tinyurl.com/yhkwtd>
<http://www.nytimes.com/2006/11/10/us/politics/10florida.html>
<http://www.lipsio.com/SarasotaFloridaPrecinct22IncidentPhotos/>

Il valore delle elezioni sabotate:

<http://www.schneier.com/essay-046.html>

La percezione:

<http://www.npr.org/templates/story/story.php?storyId=6449790>

Il "dirottamento" dei votanti:

<http://blackprof.com/stealingd.html>

Obblighi di identificazione:

<http://www.lwvwi.org/cms/images/stories/PDFs/VR%20Photo%20ID.pdf>
<http://www.demos.org/page337.cfm>

Una striscia di Foxtrot sull'argomento:

<http://www.gocomics.com/foxtrot/2006/10/29>

Anche Avi Rubin ha scritto per "Forbes" un ottimo articolo sul voto.

http://www.forbes.com/home/free_forbes/2006/0904/040.html

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

Ancora sulle macchine per il voto elettronico

Florida 13 si sta rivelando un problema ben più grande di quanto io abbia accennato:

"Il candidato Democratico, Christine Jennings, ha perduto nei confronti del suo avversario, il Repubblicano Vern Buchanan, con uno scarto di soli 373 voti su un totale di 237.861, uno dei testa a testa elettorali amministrativi più ravvicinati del paese. Più di 18.000 elettori di Sarasota County, ossia il 13% di coloro che si sono recati alle urne martedì, pare non abbiano votato per le elezioni politiche secondo quanto risulta dai voti raccolti, una discrepanza che Kathy Dent, il sovrintendente elettorale della contea, ha dichiarato di non saper spiegare.

"A confronto, soltanto il 2% dei votanti di una vicina contea facente parte dello stesso distretto amministrativo, e il 5% di un'altra hanno omesso il voto politico, secondo lo Herald Tribune di Sarasota. E molti di coloro che apparentemente non hanno votato per le amministrative risultano aver votato in gare elettorali molto più remote, come quella

per il consiglio ospedaliero."

E i voti per corrispondenza raccolti per la medesima gara elettorale mostrano solamente una differenza del 2,5% nel numero di persone che hanno votato per candidati di altre gare elettorali ma non per il Congresso.

Sarà effettuato un riconteggio, e con un margine così ravvicinato non si sa davvero chi vincerà alla fine. Ma dato che un numero così grande di voti non è stato registrato (e non vedo come chiunque abbia un minimo di conoscenze in ambito statistico possa esaminare questi dati senza concludere che tali voti non sono stati registrati), non sapremo mai chi meriterebbe realmente la vittoria elettorale in questo distretto.

In Pennsylvania, il Republican State Committee ha chiesto al Segretario di Stato di sequestrare le macchine per il voto a causa di potenziali errori di voto. Secondo KDKA:

"Funzionari del GOP della Pennsylvania hanno dichiarato che, secondo alcune voci, alcune macchine hanno trasformato i voti Repubblicani in voti Democratici. Hanno quindi richiesto allo stato di indagare e non escludono un ricorso legale per l'invalidazione della votazione.

"Secondo la fazione di Santorum, la gente sta votando per Santorum, ma il voto viene registrato come non valido o a favore di Casey."

RedState.com descrive alcuni dei problemi:

"RedState sta ricevendo una gran quantità di notizie su un incubo elettorale che sta prendendo forma in Pennsylvania a causa di certi modelli di macchine per il voto elettronico.

"In alcune contee le macchine vanno in crash. In altre abbiamo un numero tale di resoconti da ritenere la notizia credibile, secondo cui alcuni dei voti a favore di Rendell vengono conteggiati dalle macchine come a favore di Swann e viceversa. La stessa cosa sta accadendo a Santorum e Casey. Sono state presentate istanze al Segretario di Stato della Pennsylvania, ma senza alcun esito."

Sono lieto di trovare un Repubblicano alla parte a cui tocca gestire i problemi.

Anzi, no. In realtà non mi fa piacere che a qualcuno tocchi gestire i problemi legati al voto. Ma sono stufo marcio che tale questione sia percepita come un problema di parte, e mi auguro che le perdite di qualche Repubblicano in vista che possono essere attribuite a malfunzionamenti delle macchine per il voto elettronico (o anche a una frode vera e propria) contribuiranno a cambiare tale percezione. Questo è un problema molto grave che coinvolge tutti, e porvi rimedio è nell'interesse di ognuno.

FL-13 è stato il grande disastro delle macchine per il voto, ma non è stato un caso isolato: sono stati riportati altri problemi alle macchine per il voto elettronico. La EFF ha scritto: "Le tipologie di problemi delle macchine riferite ai volontari della EFF erano assai vaste, per dimensioni ed estensione. In diversi stati, fra cui Ohio, Florida, Georgia, Virginia, Utah, Indiana, Illinois, Tennessee e California, i seggi elettorali sono stati aperti con ritardo per motivi legati alle macchine. In un seggio di Broward County (Florida) le macchine per il voto elettronico non si sono accese, e alcuni cittadini non hanno potuto votare per ore. La EFF e la Election Protection Coalition hanno cercato di tenere aperto il seggio fino a tardi per venire incontro agli elettori frustrati dai ritardi, ma i funzionari si sono rifiutati. A

Utah County (Utah), più di 100 distretti elettorali hanno aperto con una-due ore di ritardo a causa di problemi alle macchine per il voto. I funzionari elettorali sia provinciali che statali si sono rifiutati di tenere aperti i seggi più a lungo per recuperare il tempo perduto, e un giudice ha persino respinto la richiesta di un elettore per un'estensione oraria, richiesta che era stata consegnata dalla EFF."

E in un'elezione comunale uno dei candidati ha ricevuto zero voti, sebbene egli sia assolutamente certo di aver votato per se stesso.

Anche ComputerWorld sta riportando problemi in varie parti del paese; stesso dicasi per il New York Times. Avi Rubin, i cui scritti sulla sicurezza del voto elettronico sono sempre letture consigliate, parla della situazione di cui è stato testimone nel Maryland:

"L'elettore aveva effettuato le sue scelte e aveva premuto il pulsante "conferma voto" sulla macchina. La macchina aveva espulso la sua smartcard, come da procedura, ma a video era rimasta la schermata riassuntiva, e non appariva alcuna registrazione del suo voto. L'elettore ha quindi reinserito la smartcard, e la macchina ha reagito dicendo che egli aveva già votato. Ma, allo stesso tempo, la persona si trovava di fronte la schermata che appare durante la procedura di voto. L'elettore allora ha premuto un'altra volta il pulsante "conferma voto", ed è comparso a video un errore che lo invitava a richiedere assistenza a un giudice. L'elettore ha dimostrato molta pazienza, ma chiaramente stava anche prendendo la situazione molto sul serio, come ci si aspetterebbe. Dopo aver discusso con lui i dettagli su quanto accaduto con molta attenzione, era mia opinione che tale macchina avesse presentato una qualche anomalia, e che si era ritrovata in una condizione imprevista dopo aver espulso la smartcard. La questione che abbiamo dovuto affrontare a quel punto era se il suo voto era stato registrato o meno. Secondo la macchina i voti registrati erano 145. Pertanto ho suggerito di contare le tessere di autorizzazione al voto che si trovavano nella busta attaccata alla macchina. Dato che le stavamo suddividendo in gruppi di 25 durante la giornata, il conteggio è stato molto semplice, e abbiamo scoperto che le tessere erano 146. Questo poteva significare due cose: che il voto di quell'elettore non era stato registrato, o che il conteggio era sbagliato per qualche altro motivo. Considerando che il conteggio di quella specifica macchina era stato perfetto fino a quel momento, ho ritenuto assai probabile che l'anomalia risiedesse nella mancata registrazione di quel voto. Purtroppo (dato che nel frattempo tutti gli altri elettori se n'erano già andati) altri giudici elettorali avevano rimosso e archiviato i registri del voto elettronico, e non vi era alcun modo di codificare un'altra smartcard per questo votante. L'unica possibilità rimasta era quella di far votare l'elettore mediante una scheda provvisoria, e così si è fatto. Questa persona è stata molto disponibile e ha compreso il nostro impiccio.

"Il fatto è che non sono sicuro se il voto di questo elettore verrà conteggiato una o due volte (o se non sarà conteggiato affatto, se il comitato elettore respingerà la sua scheda provvisoria). Infatti, lo scopo di contare le tessere di autorizzazione al voto è quello di verificare i conteggi delle macchine ogni ora. Ciò che abbiamo fatto è stato utilizzare il numero di tessere per dedurre se un determinato elettore avesse votato oppure no, e questa è un'informazione che le tessere non possono fornire direttamente. Purtroppo ritengo che esista una quantità inimmaginabile di problemi legati a queste macchine, situazioni in cui non è possibile sapere con certezza se il voto di un elettore è stato registrato o meno, e le macchine non offrono alcun sistema per effettuare dei controlli in tal senso. Se avessimo delle schede cartacee conteggiate da scanner ottici, inghippi del genere non si presenterebbero."

Quante centinaia di storie simili sono necessarie prima di concludere che le macchine per il voto elettronico non sono strumenti sufficientemente accurati per le elezioni?

C'è di buono che i problemi di FL-13 hanno convinto alcuni dei precedenti oppositori in quel distretto: "Il sovrintendente elettorale Kathy Dent ora sostiene che soddisferà la richiesta degli elettori in merito a un nuovo sistema di voto, un sistema che possa generare una traccia cartacea. [...] Il suo annuncio di venerdì indica un'inversione di rotta per il sovrintendente, che fino a quel momento aveva strenuamente difeso il sistema touch-screen acquistato dalla contea nel 2001 per 4,5 milioni di dollari."

Uno dei commenti più stupidi che mi capita di sentire in merito al voto elettronico si esprime più o meno in questi termini: "Se si possono proteggere transazioni finanziarie dell'ordine di milioni di dollari, si dovrebbe poter essere in grado di proteggere il sistema di voto". La maggior parte della sicurezza in ambito finanziario è possibile grazie all'auditing: i nomi sono legati a ogni transazione, e le transazioni possono essere dipanate ed esaminate una per una in caso di problemi. Il sistema di voto prevede una scheda anonima, e quindi la maggior parte dei sistemi antifrode del settore finanziario non si possono applicare alla realtà del voto (ho spiegato tutto questo per la prima volta nel 2001).

Nel Minnesota si utilizzano schede cartacee conteggiate da scanner ottici, e abbiamo alcune fra le elezioni meglio gestite del paese. Se fra i lettori di questa newsletter vi è qualcuno in procinto di acquistare nuove apparecchiature elettorali, adesso sa che cosa comprare.

D'altra parte sono sempre più dell'idea che la soluzione migliore sia un'elezione che avvenga al 100% per corrispondenza, come è d'uso nell'Oregon. Certo, con schede inviate per posta vi sono problematiche legate all'autenticazione, ma sono questioni da risolvere comunque, fintanto che si autorizzano i voti per corrispondenza. E sì, vi sono problematiche legate alla compravendita dei voti, ma sono generalmente considerati problemi secondari. I benefici derivati dall'insieme di 1) schede cartacee, 2) nessuna preoccupazione per eventuali code al seggio elettorale provocate da guasti o da un numero insufficiente di macchine, 3) maggiore affluenza alle urne, e 4) uno smorzamento della frenesia dell'ultimo minuto delle campagne elettorali, rendono il sistema elettorale dell'Oregon una soluzione sicuramente appetibile.

FL-13:

<http://www.nytimes.com/2006/11/10/us/politics/10florida.html>
<http://www.srgelections.com/results/gen2006sum.htm>
<http://www.srgelections.com/results/gen2006pct.htm>
<http://www.heraldtribune.com/apps/pbcs.dll/article?AID=/20061111/NEWS/611110643> oppure <http://tinyurl.com/ygo731>

Convincere gli oppositori:

<http://www.heraldtribune.com/apps/pbcs.dll/article?AID=/20061111/NEWS/611110530> oppure <http://tinyurl.com/yhr6uv>

La situazione in Pennsylvania:

http://kdka.com/topstories/local_story_311194635.html
http://www.redstate.com/stories/elections/2006/breaking_massive_meltdown_in_pennsylvanian oppure <http://tinyurl.com/yjrb68>

http://www.eff.org/news/archives/2006_11.php#004991
<http://www.computerworld.com/action/article.do?command=viewArticleBasic>

"Ma anche in un riconteggio assolutamente cristallino non vi è sempre una risposta sicura. Avete mai contato un barattolo di monetine? Lo avete fatto una seconda volta? E lo avete fatto fare a un amico, dopo? Avete sempre ottenuto il medesimo risultato? Oppure avete semplicemente fatto una media dei vari risultati? Se siete come me, probabilmente vi accordate su una quantità media. Il concetto basilare qui è che ogni elezione, come quei riconteggi del barattolo di monetine, assomiglia più a un sondaggio su un elettorato"

Conley ha ragione, ma è più complicato di così.

Esistono due tipologie essenziali di errori di voto: errori casuali ed errori sistemici. Gli errori casuali sono, appunto, casuali. I voti a favore di A attribuiti per errore a B sono probabili quanto i voti a favore di B attribuiti per errore ad A. Questo è il motivo per cui, tradizionalmente, è improbabile che i riconteggi in gare elettorali serrate finiscano col cambiare di molto le cose. Il riconteggio rivelerà una minima percentuale di errori in entrambe le direzioni, e si annulleranno a vicenda. Ma in una gara elettorale molto serrata, un attento riconteggio darà un risultato molto più accurato (anche se, per certo, non perfettamente accurato).

Gli errori sistemici sono più importanti, perché faranno in modo che i voti a favore di A saranno attribuiti a B secondo un rapporto diverso rispetto alla situazione opposta. Tali errori possono costituire un'enorme differenza in un'elezione, perché possono facilmente spostare migliaia di voti da A a B senza che vi sia alcuno spostamento da B ad A che ristabilisca un equilibrio. Questi errori possono essere un problema specifico all'interno del sistema (una scheda mal progettata, per esempio), o un errore casuale che avviene solamente nei distretti in cui A ha maggiori sostenitori di B.

Ecco dove i problemi delle macchine per il voto elettronico si fanno critici: sono infatti molto più probabilmente problemi sistemici. Lo scambio di voti, per esempio, pare generalmente interessare un candidato più di un altro. Anche le anomalie di singole macchine andranno a ripercuotersi maggiormente sui sostenitori di un candidato piuttosto che un altro, a seconda di dove è situata quella particolare macchina. E se non esistono schede cartacee a cui fare riferimento, nessun riconteggio può rimediare a tali problemi.

Conley propone di annullare ogni elezione in cui il margine di vittoria sia minore dell'1%, e di far tornare tutti alle urne. Sono d'accordo con lui, ma credo che il suo margine sia troppo grande. Nelle elezioni per il Senato della Virginia, Allen ha fatto bene a non richiedere un riconteggio. Anche se la sua perdita di 7.800 voti rappresentava solo lo 0,33%, in assenza di errori sistemici è improbabile che un riconteggio possa cambiare le cose. Penso che abbia più senso ripetere l'elezione automaticamente se il margine di vittoria è inferiore allo 0,1%.

Ancora Conley:

"Certo, è più costoso organizzare un'elezione due volte, ma si tenga presente che già in molti luoghi si è soliti andare allo spareggio quando il candidato in testa alla gara non riesce a superare un certo valore soglia. Se siamo disposti ad affrontare una situazione del genere, perché non fare lo stesso per ottenere la certezza in un'elezione che si sta giocando sul filo del rasoio? Una possibile obiezione è che un tale piano non faccia altro che spostare l'ambito del dibattito e dell'incertezza verso una nuova soglia: la soglia del 99%. Tuttavia, quei candidati che perdono con un margine di errore hanno molto meno potere retorico per parlare di risarcimento rispetto a coloro per i quali una vera e propria maggioranza è solo questione di qualche

voto in più.

"Ammettere che il caso e che l'errore di campionamento giochino un ruolo importante nelle nostre decisioni governative può metterci a disagio da un punto di vista esistenziale; ma in realtà, richiedendo un margine di vittoria che sia maggiore di un solo voto (apparentemente arbitrario), si verrebbe a realizzare una sorta di "tampone" per la democrazia, qualcosa che possa darci una maggiore sicurezza che il 'vincitore' abbia davvero vinto".

Questa è una buona idea, ma non risolve i problemi sistemici del voto. Se esistono problemi sistemici, dovrebbe poter essere stabilita un'altra giornata elettorale solo per quei distretti in cui tali problemi si sono presentati e solo per coloro che possono dimostrare di aver votato (o di aver provato a votare, ma senza successo) durante la prima giornata elettorale. (Anche se mi sembrerebbe più sensato istituire un altro protocollo per la ripetizione del voto).

Ma soprattutto abbiamo bisogno di macchine per il voto elettronico e di procedure di voto migliori.

<http://www.nytimes.com/2006/11/06/opinion/06conley.html>

Lo scambio di voti:

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9004858&source=NLT_SEC&nid=38 oppure
<http://tinyurl.com/yfdhk6>

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

La necessità di funzionari elettorali professionali

Negli Stati Uniti, le elezioni vengono gestite da un esercito di centinaia di migliaia di volontari. Sono persone sia Democratiche sia Repubblicane, e l'idea di fondo è che un gruppo sorvegli l'altro: sicurezza basata sul conflitto di interessi. Ma ad avere autorità sono funzionari eletti o incaricati dallo stato, e molti brogli elettorali negli ultimi anni sono stati organizzati da queste persone.

In un altro editoriale di opinione del New York Times, Richard Hansen, professore alla Loyola Law School, propone la figura di funzionari elettorali professionali e super partes: "Gli Stati Uniti dovrebbero seguire l'esempio delle democrazie avanzate del resto del mondo e affidare il compito a professionisti super partes. Sono necessarie figure la cui fedeltà sia legata fondamentalmente alla correttezza, all'integrità e alla professionalità del procedimento elettorale, e non ad aiutare questo o quel partito a ottenere un vantaggio politico. Non abbiamo bisogno che controversie come quella attualmente in corso in Florida vengano risolte da stratagemmi di parte."

E: "Per aumentare le possibilità che i vari stati scelgano un funzionario elettorale capo competente e indipendente, gli stati dovrebbero emanare leggi che rendano tale funzionario un incaricato del governo a lungo termine che entri in carica solo a seguito di una conferma da parte del 75% dei voti della legislatura, un requisito di maggioranza qualificata che garantirebbe il sostegno realmente bipartitico a favore del candidato. L'imparzialità nell'ambito dell'amministrazione elettorale non è una chimera: è il sistema utilizzato da Canada e Australia per gestire le proprie elezioni."

A mio avviso, tutto questo è molto più facile in teoria che non in

pratica. Tutte queste centinaia di migliaia di funzionari elettorali disinteressati, da dove verranno? E come possiamo assicurarci che essi siano realmente corretti e imparziali, e non semplicemente dei partigiani sotto mentite spoglie? Continuo a preferire la sicurezza per conflitto d'interessi.

Ma gradisco molto anche l'idea di Hansen di una figura di funzionario elettorale capo designato da una maggioranza qualificata per ogni stato. Per lo meno Hansen sta dando il via al dibattito sulla ricerca di migliori procedure elettorali per gli Stati Uniti.

<http://www.nytimes.com/2006/11/11/opinion/11hasen.html>

** *** *****

Rischio percepito e rischio effettivo

Ho scritto più volte in merito alla differenza fra rischio percepito e rischio effettivo, e di come serva a comprendere molti compromessi di sicurezza apparentemente fuori luogo. Ecco un editoriale di opinione del Los Angeles Times che fa lo stesso. L'autore è Daniel Gilbert, professore di psicologia ad Harvard (ho appena finito di leggere il suo libro "Stumbling on Happiness", che non è un volume di auto-aiuto, ma tratta di come funziona il cervello - lettura fortemente consigliata).

Il pezzo di Gilbert riguarda la reazione del pubblico ai rischi legati al riscaldamento globale e al terrorismo, ma gli argomenti che propone sono di natura più generale. Egli fornisce quattro motivazioni per cui alcuni rischi vengono percepiti come più o meno seri di quanto sono in realtà:

1. Si reagisce in maniera eccessiva nei confronti di azioni deliberate, e si tende a minimizzare incidenti, eventi astratti e fenomeni naturali. "Per questo ci si preoccupa molto di più dell'antrace (con un numero annuale di vittime pari a circa zero) che non dell'influenza (con un numero annuale di vittime che va da 250.000 al mezzo milione). L'influenza è un accidente naturale, l'antrace è un'azione intenzionale, e l'azione più piccola attira l'attenzione molto più dell'accidente di più grande portata. Se due aeroplani fossero stati colpiti da un fulmine e si fossero schiantati in un grattacielo di New York, poche persone sarebbero state in grado di ricordare la data di quell'avvenimento."

2. Si reagisce in maniera eccessiva nei confronti di cose che offendono la morale. "Quando le persone si sentono insultate o qualcosa le disgusta, generalmente si mettono in azione, prendendosi a bastonate o andando a votare. Le emozioni morali sono l'ordine di entrare in azione impartito dal cervello."

Gilbert non lo dice, ma è ragionevole assumere che si tende a non reagire di fronte a cose che non offendono la morale.

3. Si reagisce in maniera eccessiva verso minacce immediate, mentre quelle a lungo termine vengono generalmente sottovalutate. "Il cervello è una macchina meravigliosamente congegnata per evitare ostacoli, che analizza costantemente l'ambiente circostante alla ricerca di ostacoli da schivare qui e ora. Questo è ciò che ha fatto il cervello per svariate centinaia di milioni di anni; poi, a un certo punto, solo qualche milione di anni fa, il cervello dei mammiferi ha imparato un nuovo stratagemma: prevedere il momento e la posizione di un pericolo prima che questo si manifesti. La nostra capacità di evitare ciò che non si sta ancora presentando è una delle innovazioni più sbalorditive del

nostro cervello, e senza di essa non avremmo il filo interdentale o i piani di previdenza. Ma tale innovazione è ancora nelle prime fasi di sviluppo. L'applicazione che ci permette di reagire nei confronti di palle da baseball ben visibili è antica e affidabile, però l'utility aggiuntiva che ci consente di rispondere a minacce che incombono in un futuro ancora invisibile è tuttora in fase beta, per così dire."

4. Si tende a non reagire di fronte a cambiamenti che avvengono lentamente e nel tempo. "Il cervello umano è squisitamente sensibile a variazioni di luce, suono, temperatura, pressione, dimensioni, peso e praticamente ogni altra cosa. Ma se il tasso di cambiamento è sufficientemente lento, il cambiamento passerà inosservato. Se il basso mormorio di un frigorifero dovesse aumentare in altezza nel giro di parecchie settimane, quell'elettrodomestico potrebbe cantare in tonalità soprano alla fine del mese e nessuno farebbe una piega."

È interessante confrontare tutto questo con ciò che ho scritto in "Beyond Fear" (pagg. 26-27) sul rischio percepito e il rischio effettivo:

" * Le persone ingigantiscono rischi spettacolari ma rari e sminuiscono i rischi più comuni. Si preoccupano molto di più per i terremoti che non di scivolare sul pavimento del bagno, anche se quest'ultimo fa molte più vittime del primo. Analogamente, il terrorismo provoca molta più ansietà dei reati della criminalità comune, anche se quest'ultima miete più vittime del primo. Molte persone ritengono che durante la festa di Halloween i propri figli corrano il rischio di ricevere caramelle avvelenate da estranei, malgrado non esista un solo caso documentato a fondamento di questa paura.

" * Le persone hanno difficoltà a calcolare i rischi legati a qualsiasi scenario che si discosta dalla loro situazione normale. Gli americani si preoccupano molto più del rischio di aggressioni e furti in una città straniera, a prescindere da quanto tale città possa essere più sicura di quella in cui vivono. Gli europei periodicamente hanno la percezione che negli Stati Uniti vi siano pistole in ogni dove. Gli uomini sottovalutano continuamente quanto possa essere rischiosa una situazione per una donna non accompagnata. I rischi di crimini informatici di solito vengono ingigantiti perché i computer sono strumenti relativamente nuovi e i rischi a essi legati poco conosciuti. Gli americani appartenenti al ceto medio possono essere particolarmente ingenui e contenti di sé; le loro vite sono incredibilmente sicure per la maggior parte del tempo, e quindi i loro istinti nei confronti dei rischi di molte situazioni sono andati attenuandosi.

" * I rischi personificati vengono percepiti come più gravi di quelli anonimi. Stalin disse 'Una sola morte è una tragedia, un milione di morti sono una statistica'. Aveva ragione: i grandi numeri hanno la tendenza a mescolarsi fra loro. Il numero definitivo delle vittime dell'11 settembre è stato minore della metà delle stime iniziali, ma ciò non ha portato la gente a sentirsi meno a rischio. Le persone si perdono in commenti sulle statistiche delle morti causate da incidenti d'auto, ma quando la stampa scrive pagine e pagine sulla vicenda di nove individui intrappolati in una miniera (completa di storie commoventi sulle loro vite e sulle loro famiglie), ecco che immediatamente il pubblico inizia a rendersi conto dei pericoli con i quali i minatori hanno avuto a che fare per secoli. Osama Bin Laden rappresenta il volto di Al Qaeda, ed è stato utile come personificazione della minaccia terroristica. Anche se fosse morto, servirebbe gli interessi di alcuni politici mantenerlo "vivo", dato il suo effetto sull'opinione pubblica.

" * Le persone sottovalutano i rischi che decidono di correre volontariamente e sopravvalutano i rischi legati a situazioni che non

La sicurezza dei "controlli ed equilibri" (Checks and Balances):
<<http://www.schneier.com/crypto-gram-0411.html#10>>

Security Information Management Systems (SIMS):
<<http://www.schneier.com/crypto-gram-0411.html#12>>

Tecnologia e lotta al terrorismo:
<<http://www.schneier.com/crypto-gram-0411.html#13>>

Gli hacker degli aerei:
<<http://www.schneier.com/crypto-gram-0311.html#1>>

La difesa del Trojan:
<<http://www.schneier.com/crypto-gram-0311.html#8>>

Esposizione totale:
<<http://www.schneier.com/crypto-gram-0111.html#1>>

Perché le Firme Digitali non sono delle Firme
<<http://www.schneier.com/crypto-gram-0011.html#1>>

Programmare il computer di Satana, ovvero: perché i computer non sono sicuri:
<<http://www.schneier.com/crypto-gram-9911.html#WhyComputersareInsecure>>
oppure <<http://tinyurl.com/7ldrl>>

La crittografia a chiave pubblica basata sulla matematica delle curve ellittiche (Elliptic Curve Cryptography):
<<http://www.schneier.com/crypto-gram-9911.html#EllipticCurvePublic-KeyCryptography>> oppure <<http://tinyurl.com/a2low>>

Il futuro della frode: tre motivi che spiegano perché il commercio elettronico è diverso.
<<http://www.schneier.com/crypto-gram-9811.html#commerce>>

La protezione anti-copia del software e perché non funziona:
<<http://www.schneier.com/crypto-gram-9811.html#copy>>

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

Il programma Total Information Awareness è tornato

Vi ricordate di Total Information Awareness (TIA), l'enorme database contenente informazioni su tutti quanti, che avrebbe dovuto contribuire alla cattura di terroristi? Il pubblico lo trovò talmente aberrante, e si oppose con tale forza, che il Congresso tagliò i fondi per il programma nel settembre 2003.

Nessun esperto di sicurezza credette che quella sarebbe stata davvero la fine di TIA. Pensammo invece che sarebbe stato trasformato in un programma segreto e gli sarebbe stato affibbiato un nuovo nome. Beh, il programma ora si chiama Tangram, ed è segreto.

Il National Journal scrive:

"L'agenzia di intelligence governativa primaria sta realizzando un sistema computerizzato per esaminare vaste quantità di informazioni alla ricerca di pattern di attività che possano indicare complotti terroristici. Il sistema, gestito dall'Ufficio del Direttore dell'Intelligence Nazionale, è ai primi stadi di ricerca e viene collaudato in parte utilizzando dati di intelligence governativi che

possono contenere informazioni sui cittadini statunitensi e su altre persone che si trovano nel paese.

"Esso comprende sistemi di rilevamento e di profiling già esistenti, fra cui quelli che creano "profili di rischio" per sospetti terroristi analizzando database sterminati di dati di intelligence governativi, insieme a registri di comunicazioni private, transazioni finanziarie e altre attività giornaliere".

Le informazioni su Tangram provengono da un documento governativo che ricerca collaboratori che contribuiscano a progettare e a realizzare il sistema.

DefenseTech scrive: "Il documento, che è una descrizione del programma Tangram per potenziali collaboratori, descrive altri sistemi di rilevamento e profiling già esistenti che non si sono ancora evoluti oltre lo stadio dei cosiddetti 'modelli di colpevolezza per associazione', i quali collegano sospetti terroristi a potenziali associati, ma che apparentemente non forniscono agli analisti molte informazioni sui motivi per cui tali collegamenti siano significativi. Tangram vuole progredire rispetto a questi metodi, e anche investigare l'efficacia di altri collegamenti di rilevazione quali il 'collective inferencing', che mira a realizzare profili di rischio di interi gruppi di persone allo stesso tempo."

Il data mining antiterrorismo è sempre stata un'idea stupida. E l'esistenza di Tangram non fa che evidenziare il problema, con il Congresso che cerca di fermare un programma tagliandone i finanziamenti, e il programma che ritorna sotto un altro nome.

<http://nationaljournal.com/about/njweekly/stories/2006/1020nj3.htm>
<<http://www.fbo.gov/spg/USAF/AFMC/AFRLRRS/Reference-Number-BAA-06-04-IFK A/SynopsisP.html>> oppure <<http://tinyurl.com/y5sg9l>>
<<http://www.defensetech.org/archives/002875.html>>

I miei interventi precedenti sul data mining:

<http://www.schneier.com/blog/archives/2006/03/data_mining_for.html>
<http://www.schneier.com/blog/archives/2006/05/the_problems_wi.html>

** *** *****

Contraffare il proprio permesso di imbarco

La scorsa settimana Christopher Soghoian ha creato un sito Web contenente un generatore di biglietti d'imbarco fasulli, permettendo a chiunque di produrre una carta di imbarco della Northwest Airlines: per qualsiasi nome, aeroporto, data e volo. Questa idea gli è costata una visita dell'FBI, che in un secondo momento ha fatto irruzione in casa sua, sequestrandogli i computer e altri oggetti personali. Ciò ha provocato una serie di richieste di arresto, la più notevole da parte del Rappresentante Edward Markey (D-Massachusetts), che l'ha poi revocata. E tutta la faccenda gli ha procurato più pubblicità di quanta si sarebbe mai sognato.

Tutto per dimostrare un'ovvia e ben nota vulnerabilità della sicurezza aeroportuale che riguarda i biglietti di imbarco e i documenti di identità.

Tale vulnerabilità non rappresenta nulla di nuovo. Vi è un articolo su CSOnline del febbraio 2006. Vi è un articolo su Slate del febbraio 2005. Il senatore Chuck Schumer ne ha parlato nel 2005. Io ne scrissi

nel numero di Crypto-Gram dell'agosto 2003. È possibile che io sia stata la prima persona a pubblicare qualcosa a riguardo, ma certamente non sono stato il primo a pensare a un'idea del genere.

È davvero lapalissiano: se si riesce a creare una carta di imbarco fasulla, con essa si può oltrepassare il checkpoint di sicurezza. Bella scoperta, lo sappiamo tutti.

Si può anche utilizzare un permesso di imbarco falso per volare con un biglietto aereo altrui. Lo stratagemma consiste nell'avere due biglietti di imbarco: uno legittimo, con il nome di chi ha prenotato, e un altro fasullo che riporta lo stesso nome del vostro documento di identità con foto. La carta di imbarco falsa vi servirà per passare oltre la sicurezza, e il biglietto vero e proprio a nome di qualcun altro per imbarcarvi sull'aereo.

Questo significa che un terrorista il cui nome sia presente sulla no-fly list può volare senza problemi: compra un biglietto a nome di qualcun altro, magari usando una carta di credito rubata, e si serve del proprio documento d'identità e del permesso di imbarco fasullo per oltrepassare la sicurezza in aeroporto. Dato che il permesso è a nome di un innocente, non farà scattare nessun segnale di pericolo sulla no-fly list.

È anche possibile servirsi di un permesso di imbarco fasullo invece di quello vero se avete il marchio "SSSS" e volete evitare lo screening secondario, oppure se non siete in possesso di un biglietto e intendete accedere alla zona di imbarco.

Storicamente, la falsificazione di un permesso di imbarco è sempre stata un'operazione difficile, in quanto era necessario dotarsi di carta e attrezzature speciali. Ma da quando l'Alaska Airlines ha lanciato l'idea nel 1999, moltissime linee aeree oggi permettono ai passeggeri di stamparsi il proprio permesso di imbarco con il computer di casa, per poi portarlo con sé in aeroporto. Questo programma fu temporaneamente sospeso dopo l'11 settembre, ma fu subito ripristinato a seguito di pressioni da parte delle stesse linee aeree. Le persone che stampano il proprio permesso di imbarco a casa possono recarsi direttamente al checkpoint di sicurezza in aeroporto, e ciò significa impiegare meno personale.

Le linee aeree generano i permessi di imbarco come file grafici, il che vuol dire che chiunque abbia un minimo di dimestichezza con un programma di fotoritocco come Photoshop è in grado di modificarli. Tutto quel che faceva il sito Web di Soghoian era automatizzare il processo usando i permessi di imbarco di una sola compagnia aerea.

Soghoian afferma che le sue intenzioni erano di dimostrare la vulnerabilità. Possiamo dire che lo ha fatto in una maniera un po' stupida, ma non credo che quel che ha fatto sia sostanzialmente peggiore di quanto io scrissi nel 2003, o di quanto ha descritto Schumer nel 2005. Perché chi dimostra la vulnerabilità viene accusato e diffamato, mentre chi la descrive viene praticamente ignorato? O, ancora peggio, perché l'organizzazione che causa quella vulnerabilità viene ignorata? Perché accanirsi contro il messaggero invece di discutere il problema?

Come ho scritto nel 2005: "La vulnerabilità è ovvia, ma i concetti generali lo sono meno. Vi sono tre elementi da autenticare: l'identità del passeggero, il permesso di imbarco e il registro sul computer. Immaginatoli come i tre vertici di un triangolo. Con il sistema attuale, il permesso di imbarco viene confrontato con l'identità del passeggero, poi il permesso di imbarco viene confrontato con il registro sul computer. Ma dato che il documento di identità non viene mai

confrontato con il registro sul computer (il terzo lato del triangolo), è possibile creare due permessi di imbarco diversi senza che nessuno se ne accorga. Ecco perché l'attacco funziona."

Il modo per sistemare il problema è altrettanto ovvio: verificare l'accuratezza dei permessi di imbarco ai checkpoint di sicurezza. Se i passeggeri dovessero far passare i permessi di imbarco sotto uno scanner durante i controlli di sicurezza, il computer potrebbe verificare che il permesso di imbarco, che già conferma i dati del documento di identità con foto, coincida anche con i dati presenti nel computer. Si chiuda il triangolo dell'autenticazione, e la vulnerabilità scomparirà.

Ma prima di iniziare a investire tempo e denaro e agenti della TSA, diciamocelo in tutta onestà: l'obbligo del documento di identità con foto non è altro che una messinscena di sicurezza. Il suo unico scopo di sicurezza è quello di confrontare i nominativi con quelli presenti nella no-fly list, che sarebbe comunque una cosa ridicola anche se non fosse così facile da aggirare. L'identificazione, in questo contesto, non è un'utile misura di sicurezza.

È piuttosto interessante notare come, malgrado l'obbligo del documento di identità con foto venga presentato come una misura di sicurezza antiterrorismo, esso sia in realtà una misura di sicurezza commerciale delle compagnie aeree. Fu adottata per la prima volta nel 1996, dopo l'esplosione del volo 800 della TWA sull'Atlantico. Il governo all'inizio pensò che la causa fosse un attentato terroristico, ma fu poi dimostrato che si trattò di un tragico incidente.

A differenza di ogni altra misura di sicurezza aerea (fra cui il rinforzo delle porte di accesso alla cabina di pilotaggio, che avrebbe potuto prevenire l'attentato dell'11 settembre), le compagnie aeree non hanno opposto resistenza all'obbligo del documento di identità, perché ha risolto un problema commerciale: la rivendita di biglietti non rimborsabili. Prima che vi fosse la richiesta di presentazione di un documento, biglietti del genere venivano continuamente proposti nelle pagine degli annunci: "Viaggio andata e ritorno, New York-Los Angeles, dal 21 al 30 novembre, passeggero di sesso maschile, 100 dollari". Dato che le linee aeree non controllavano le carte di identità, chiunque fosse del sesso giusto poteva utilizzare il biglietto. Le compagnie aeree non gradivano la cosa, e hanno cercato più volte di chiudere quel mercato. Nel 1996 sono finalmente riuscite a risolvere il problema, addossando la colpa alla FAA e al terrorismo.

E quindi la ragione principale per cui è in vigore l'obbligo del documento di identità è il commercio, ed è proprio a causa del commercio che è possibile aggirare tale obbligo con facilità. Invece di perseguire una persona che dimostra una vulnerabilità evidente e già nota al pubblico, sarebbe preferibile concentrarsi sulle organizzazioni di fatto responsabili per questa falla di sicurezza e che non sono state in grado di porvi rimedio in tutti questi anni. Dov'è la risposta della TSA alla questione?

Il problema è reale, e il Dipartimento per la Sicurezza Nazionale e la TSA dovrebbero sistemare la sicurezza o scartare del tutto il sistema. Quel che abbiamo ora è il peggior sistema di sicurezza di tutti, perché rappresenta una seccatura per le persone innocenti ed è incapace di fermare i colpevoli.

Questo è il mio trentesimo articolo per Wired.com:
<<http://www.wired.com/news/columns/0,72045-0.html>>

Le notizie:
<<http://john4d4m5.bravehost.com>>

<http://slightparanoia.blogspot.com/2006/10/post-fbi-visit.html>
<http://slightparanoia.blogspot.com/2006/10/fbi-visit-2.html>
http://blog.wired.com/27bstroke6/2006/10/congressman_ed_.html
<http://markey.house.gov/index.php?option=content&task=view&id=2336&Itemid=125>> oppure <http://tinyurl.com/ymjkxa>
http://blog.wired.com/27bstroke6/2006/10/boarding_pass_g.html

Vecchi articoli riguardanti la vulnerabilità:

<http://www.csoonline.com/read/020106/caveat021706.html>
<http://www.slate.com/id/2113157/fr/rss/>
http://www.senate.gov/~schumer/SchumerWebsite/pressroom/press_releases/2005/PR4123.aviationsecurity021305.html> oppure
<http://tinyurl.com/yzoon6>
<http://www.schneier.com/crypto-gram-0308.html#6>

No-fly list:

http://www.schneier.com/blog/archives/2005/12/30000_people_mi.html
http://www.schneier.com/blog/archives/2005/09/secure_flight_n_1.html
http://www.schneier.com/blog/archives/2006/10/nofly_list.html
http://www.schneier.com/blog/archives/2005/08/infants_on_the.html

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

News

Questo articolo sostiene che la maggior parte dei 44 miliardi di dollari che gli Stati Uniti hanno investito nella difesa contro il bioterrorismo sia stato denaro sprecato.

<http://www.newscientist.com/channel/opinion/mg19225725.000>

Il futuro del malware è rappresentato da cavalli di Troia mirati:

http://news.com.com/The+future+of+malware+Trojan+horses/2100-7349_3-6125453.html> oppure <http://tinyurl.com/w8hx7>

FixAVote.com: un'ottima burla.

<http://www.fixavote.com/>
http://www.infoworld.com/article/06/10/26/HNfixelections_1.html

Intervista con un esperto borsaiolo:

<http://www.kiplinger.com/personalfinance/magazine/archives/2006/11/mystory.html>> oppure <http://tinyurl.com/y3n2ap>

La polizia svizzera sta considerando di utilizzare cavalli di Troia per effettuare intercettazioni VoIP:

<http://www.pcpro.co.uk/news/95394/swiss-look-to-trojan-code-for-voip-tapping.html>> oppure <http://tinyurl.com/ygq43m>

Pessima installazione di sicurezza domestica. (Sì, si tratta di pubblicità, ma nel post del blog vi sono delle importanti lezioni di sicurezza).

http://providentsecurity.typepad.com/community_security_the_pr/2006/10/criminal_instal.html> oppure <http://tinyurl.com/ygve7r>

Non credo di aver mai letto prima d'ora un articolo che parla di differenze di classe sociale e del loro legame con le problematiche di sicurezza.

<http://redtape.msnbc.com/2006/10/doublestandards.html>

Questo interessante pezzo del New York Times dimostra che il problema della salvaguardia e della sicurezza agricole rispecchia le problematiche di sicurezza delle reti informatiche, specialmente

considerando la monocoltura per quanto concerne sistemi operativi e protocolli di rete.

http://www.nytimes.com/2006/10/15/magazine/15wwln_lede.html
http://www.schneier.com/blog/archives/2006/08/security_and_mo.html

Una riflessione affascinante: "Warning Signs for Tomorrow" [Segnali d'allarme per il futuro].

http://www.aleph.se/andart/archives/2006/10/warning_signs_for_tomorrow.html oppure <http://tinyurl.com/yylq69>

Ottimo scritto sul rischio percepito e il rischio effettivo. Il pretesto è la richiesta del sindaco Daley di Chicago di una zona di non volo sopra l'area cittadina alla luce dell'incidente aereo a New York.

<http://www.aopa.org/whatsnew/newsitems/2006/061013enough.html>

E, sempre sullo stesso argomento, un pezzo sul perché non ha senso bandire dalle città velivoli di piccole dimensioni come misura antiterrorismo.

<http://www.salon.com/tech/col/smith/2006/10/20/askthepilot205/index.html> oppure <http://tinyurl.com/yh7nz6>

Il post sul mio blog:

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

Doonesbury sul terrorismo e la paura:

http://www.doonesbury.com/strip/dailydose/index.html?uc_full_date=20061015 oppure <http://tinyurl.com/yffbq4>

http://www.doonesbury.com/strip/dailydose/index.html?uc_full_date=20061016 oppure <http://tinyurl.com/ylwj4j>

http://www.doonesbury.com/strip/dailydose/index.html?uc_full_date=20061017 oppure <http://tinyurl.com/y76864>

http://www.doonesbury.com/strip/dailydose/index.html?uc_full_date=20061018 oppure <http://tinyurl.com/yfq9sp>

http://www.doonesbury.com/strip/dailydose/index.html?uc_full_date=20061019 oppure <http://tinyurl.com/ye2km5>

http://www.doonesbury.com/strip/dailydose/index.html?uc_full_date=20061020 oppure <http://tinyurl.com/yfbne8>

http://www.doonesbury.com/strip/dailydose/index.html?uc_full_date=20061021 oppure <http://tinyurl.com/yefhz7>

Un articolo veramente interessante sui forum hacker online, soprattutto sulla politica al loro interno.

http://www.usatoday.com/tech/news/computersecurity/infotheft/2006-10-11-cybercrime-hacker-forums_x.htm oppure <http://tinyurl.com/y8jqbv>

Un reato di ingegneria sociale nel mondo reale:

http://www.theregister.co.uk/2006/10/20/easynet_brick_lane_robbery/

Ecco un'altra vicenda di ingegneria sociale (il link è in turco). La polizia riceve una chiamata anonima di emergenza da parte di qualcuno che sostiene di aver sistemato un ordigno esplosivo all'Haydarpasa Numune Hospital. L'ospedale viene fatto evacuare (100 pazienti più i medici, il personale, i visitatori, ecc.) e si effettuano ricerche per due ore. La polizia non trova nulla. Quando pazienti e visitatori rientrano, scoprono di essere stati derubati dei loro oggetti di valore.

<http://www.milliyet.com.tr/2006/10/25/yasam/ayas.html>

Un paramedico viene fermato dalla sicurezza aeroportuale: aveva addosso dei residui di nitroglicerina. (Almeno sappiamo che quei rilevatori di residui chimici funzionano).

<http://dochazmat.livejournal.com/31044.html>

Se ci si impadronisce di una rete di computer (infettandoli con un qualche malware), la parte difficile è mantenerne il controllo.

Tradizionalmente tali computer (detti zombie) vengono controllati via

IRC, ma IRC può essere rilevato e bloccato, e quindi gli hacker si sono adeguati:

http://news.com.com/Zombies+try+to+blend+in+with+the+crowd/2100-7349_3-6127304.html oppure <http://tinyurl.com/swrbg>

Qui lo stratagemma è impedire che il legittimo proprietario del computer si accorga che qualcun altro lo sta controllando. È un continuo braccio di ferro fra aggressore e difensore.

Sigilli di garanzia:

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

<http://pearl1.lanl.gov/seals/default.htm>

Le "Privacy Guidelines for Developing Software and Services" [Linee Guida per lo Sviluppo di Software e Servizi] di Microsoft. Il documento è piuttosto buono, in effetti.

<http://www.microsoft.com/downloads/details.aspx?FamilyID=c48cf80f-6e87-48f5-83ec-a18dlad2fclf&displaylang=en>

oppure <http://tinyurl.com/y45oge>

Le "Guidelines for Identification and Authentication" [Linee Guida per l'Identificazione e l'Autenticazione] canadesi, pubblicate dal Garante per la protezione della Privacy del Canada, sono un ottimo documento che tratta sia dei rischi della privacy sia delle minacce di sicurezza.

http://www.privcom.gc.ca/information/guide/auth_061013_e.asp

E qui si può trovare un documento più lungo pubblicato nel 2004 da Industry Canada: "Principles for Electronic Authentication" [Principi per l'Autenticazione Elettronica].

http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/h_gv00240e.html

Il post nel mio blog:

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

Sorveglianza come arte performativa:

<http://www.worldchanging.com/archives/005105.html>

È una cosa estrema, ma tale livello di sorveglianza diventerà probabilmente la norma. Non si troverà in un sito Web accessibile dal pubblico, ma sarà a disposizione di governi e aziende.

Articolo di "Mother Jones" su Google e la privacy:

<http://www.motherjones.com/news/feature/2006/11/google.html>

Potranno anche essere bravi a impedirvi di portare con voi una bottiglia d'acqua sull'aereo, ma quando si tratta di individuare bombe e armi da fuoco non sono un granché: "La scorsa settimana, gli screener del Newark Liberty International Airport, uno dei punti di partenza dei dirottatori dell'11 settembre, hanno fallito 20 dei 22 test di sicurezza condotti da agenti USA sotto copertura, non accorgendosi di bombe e pistole tenute nascoste ai checkpoint di sicurezza dei tre terminal del grande punto di raccordo aereo, secondo quanto riportato da funzionari federali di sicurezza".

http://www.rawstory.com/showoutarticle.php?src=http%3A%2F%2Fseattletimes.nwsources.com%2Fhtml%2Fnationworld%2F2003327485_screeners28.html

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

Come ho già scritto in precedenza, questo è un problema davvero difficile da risolvere:

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

Si tenga presente questa verità: non è possibile tenere le armi fuori dalle prigioni, men che meno dagli aeroporti.

Il Data Privacy and Integrity Advisory Committee del Dipartimento per la Sicurezza Nazionale si è dichiarato contrario all'introduzione di chip RFID nelle carte d'identità. Il rapporto è ancora in stato di bozza, ma ciò che contiene è talmente controverso che il voto sul rapporto finale è stato rinviato.

http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_rpt_rfid_draft.pdf> oppure <http://tinyurl.com/y3k2w6>
<http://www.wired.com/news/technology/1,72019-0.html>>

Furto d'identità online: la vicenda ha, guarda caso, toni sensazionalistici.

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9004429>> oppure <http://tinyurl.com/y8mvoz>

Il CEO di un'azienda è stato arrestato per aver commesso furti di identità ai danni dei suoi dipendenti:

<http://www.varbusiness.com/sections/news/breakingnews.jhtml?articleId=193500991>> oppure <http://tinyurl.com/y44w9u>

Questo tizio vuole fornire agli studenti dei libri di testo blindati, come arma di difesa in caso di sparatorie nella scuola. Storie simili non si possono inventare.

<http://www.wbir.com/news/national/story.aspx?storyid=39017>>

Un nuovo database della Dogan

a USA su camion e viaggiatori: un ennesimo programma governativo di sorveglianza su vasta scala:

<http://arstechnica.com/news.ars/post/20061103-8143.html>>

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

http://notabob.blogspot.com/2006/11/in-crosshairs_03.html>

<http://www.eff.org/deeplinks/archives/004980.php>>

http://blog.wired.com/27bstroke6/2006/11/homeland_security.html>

<http://www.washingtonpost.com/wp-dyn/content/article/2006/11/02/AR200610201810.html>> oppure <http://tinyurl.com/yl92on>

Crittografia classica con i laser. Non avendo sufficienti nozioni di fisica, non mi è possibile esprimere una valutazione.

<http://www.physorg.com/news80478394.html>>

<http://authors.library.caltech.edu/5655/>>

Il 18 agosto dello scorso anno, il worm Zotob infettò gravemente i computer del Dipartimento per la Sicurezza Nazionale, in particolar modo le 1.300 workstation su cui girava l'applicazione US-VISIT alle frontiere. Wired News ha compilato una richiesta FIA (Freedom of Information Act) per conoscerne i dettagli. La richiesta fu respinta, e allora è stata sporta denuncia. Alla fine il governo è stato costretto a produrre i documenti. I dettagli non rivelano nulla per quanto riguarda il profilo tecnico dei sistemi informatici, e puntano soltanto all'incompetenza del Dipartimento nella gestione dell'incidente.

<http://www.wired.com/news/technology/0,72051-0.html>>

Seagate ha annunciato un prodotto chiamato DriveTrust, che fornisce una crittografia hardware sul disco stesso. La tecnologia è proprietaria, ma vengono utilizzati algoritmi standard: AES e triple-DES, RSA e SHA-1. I dettagli sulla gestione delle chiavi sono ancora vaghi, ma il sistema richiede una password di pre-boot e/o una combinazione di dati biometrici per avere accesso al disco. E Seagate sta lavorando su una sorta di sistema di gestione delle chiavi esteso all'intero ambito d'impresa, in modo che sia più semplice l'implementazione della tecnologia a livello aziendale. Il primo mercato a cui mira il prodotto sono i computer portatili. Nessun produttore di computer ha ancora annunciato il supporto per DriveTrust.

<http://www.seagate.com/cda/newsinfo/newsroom/releases/article/0,1121,3347,00.html>> oppure <http://tinyurl.com/y7tvvd>

<http://www.pcworld.com/article/id,127701/article.html>>

<http://www.theglobeandmail.com/servlet/story/RTGAM.20061030.wharddrive1029/BNStory/Technology/?page=rss&id=RTGAM.20061030.wharddrive1029>>

oppure <http://tinyurl.com/y5wtg>

http://news.com.com/Seagate+bakes+security+into+hard-disk+drive/2100-1029_3-6130824.html oppure <http://tinyurl.com/y4kzhk>
http://www.cio.com/blog_view.html?CID=26159
<http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2006/10/30/BUGU2M1ETT1.DTL> oppure <http://tinyurl.com/yjvac7>

È semplice ottenere le informazioni personali più importanti da una carta di credito con chip RFID.

<http://www.nytimes.com/2006/10/23/business/23card.html>
http://www.theregister.co.uk/2006/10/24/rfid_credit_card_hack/
<http://www.rfidjournal.com/article/articleview/2749/1/1/>

Perché i dirigenti non comprendono la sicurezza informatica:
http://www.schneier.com/blog/archives/2006/11/why_management.html

"Keyboards and Covert Channels" [Tastiere e Canali Nascosti], una ricerca interessante.
<http://www.crypto.com/papers/jbug-Usenix06-final.pdf>

"Deconstructing Information Warfare" [Decostruire l'Information Warfare]
<http://www.information-retrieval.info/PIW/deconstructing/Taipale-IW-103006.pdf> oppure <http://tinyurl.com/y2x9vt>

Il FIDIS (Future of Identity in the Information Society) non tollera i passaporti RFID:
<http://www.fidis.net/press-events/press-releases/budapest-declaration/>
<http://it.slashdot.org/it/06/11/09/1757202.shtml> oppure
<http://tinyurl.com/y4eht7>

Buon articolo sul data mining:
http://www.theregister.co.uk/2006/11/08/guilty_associations/

Una vignetta sulla crittografia: Alice, Bob, and Eve (viene anche fatto il mio nome).
<http://xkcd.com/c177.html>

Gli autonoleggi nel Regno Unito richiederanno le impronte digitali. Non sarà facoltativo, ma obbligatorio.
http://www.schneier.com/blog/archives/2006/11/uk_car_rentals.html
<http://news.bbc.co.uk/1/hi/magazine/6129084.stm>

Una Wikipedia segreta per i servizi di intelligence statunitensi:
http://news.yahoo.com/s/nm/20061031/wr_nm/internet_intelligence_dc_1

** **

La fine delle conversazioni effimere

L'infuocato dibattito politico in merito ai messaggi chat a sfondo sessuale dell'ex Rappresentante USA Mark Foley cela un'altra problematica, che riguarda la privacy. Ci stiamo rapidamente trasformando in una società in cui le nostre conversazioni private possono essere registrate e rese pubbliche in un secondo momento. Ciò rappresenta una smisurata perdita di libertà e di diritti civili, e l'unico modo di risolvere il problema è attraverso la legislazione.

Le conversazioni della sfera quotidiana sono sempre state effimere. Sia di persona che per telefono, potevamo essere ragionevolmente certi che quanto detto si sarebbe dileguato appena uscito dalle nostre bocche. Naturalmente i boss del crimine organizzato si sono sempre preoccupati di intercettazioni telefoniche e di microfoni nascosti nelle stanze, ma quella era un'eccezione. La privacy era l'assunto di base.

Le cose sono cambiate. Ora digitiamo le nostre conversazioni informali sulla tastiera di un computer. Chiacchieriamo tramite chat, email, utilizzando gli SMS dei nostri cellulari, e attraverso commenti lasciati su siti Web di social networking come Friendster, LiveJournal e MySpace. Queste conversazioni, con amici, amanti, colleghi e collaboratori, non sono per niente effimere, ma lasciano vere e proprie scie elettroniche dietro di sé.

Ne siamo coscienti a livello intellettuale, ma non abbiamo ancora interiorizzato il concetto. Continuiamo a scrivere, assorbiti dalla conversazione, dimenticandoci che tutto viene registrato.

I messaggi di Foley sono stati salvati dai giovani con cui stava comunicando, ma avrebbero potuto essere registrati anche dal servizio di messaggia istantanea. Esistono strumenti che permettono sia alle aziende che alle agenzie governative di monitorare e conservare le conversazioni di messaggia istantanea. Le email possono essere archiviate dal nostro Internet provider o dal dipartimento IT dell'azienda dove lavoriamo. Gmail, per esempio, conserva tutto, anche se lo cancellate.

E queste conversazioni possono riemergere per perseguire le persone: in procedimenti penali, cause di divorzio, o semplicemente in qualità di rivelazioni imbarazzanti. Durante il processo antitrust contro Microsoft del 1998, l'accusa esaminò enormi quantità di email, alla ricerca di prove inconfutabili. È chiaro che fu trovato qualcosa: mentre chiacchieriamo, tutti diciamo cose che possono provare qualunque altra cosa, se estrapolate dal contesto.

La morale è evidente: quel che avete scritto e poi inviato, preparatevi a spiegarlo in pubblico in futuro.

E la voce non è più un rifugio. Le conversazioni faccia a faccia sono ancora al sicuro, ma sappiamo che la National Security Agency sta controllando le chiamate internazionali di tutti i cittadini (non hanno detto nulla dei messaggi SMS, ma è ragionevole presumere che stiano monitorando anche quelli). RegISTRAZIONI periodiche di conversazioni telefoniche sono ancora rare (di certo la NSA ha i mezzi per effettuarle) ma diventeranno sempre più comuni a mano a mano che le conversazioni telefoniche si sposteranno sempre più sulla rete IP.

Se tutto questo vi turba, bene, perché dovrebbe turbarvi. Un numero sempre minore di conversazioni rimane effimero, e si sta perdendo il controllo dei dati. Affidiamo la nostra privacy al nostro Internet provider, alle aziende per cui lavoriamo, alle compagnie di telefonia cellulare, ma queste entità continuano a dimostrarsi indegne di fiducia. Ladri di identità accedono ripetutamente a questi archivi contenenti le nostre informazioni. Paris Hilton e altre celebrità sono state vittime di hacker che sono penetrati nelle reti dei loro provider di telefonia mobile. Google legge la nostra casella Gmail e inserisce annunci dipendenti dal contesto.

Ancora peggio, le comuni protezioni costituzionali non vengono applicate alla maggior parte di tutto questo. Le forze dell'ordine hanno bisogno di un mandato firmato da un giudice per ispezionare le nostre carte o per intercettare le nostre comunicazioni, ma possono limitarsi a emanare un mandato di comparizione, o a richiedere (con le buone o le cattive maniere) i nostri dati conservati presso terzi, comprese copie delle nostre comunicazioni.

Il Dipartimento di Giustizia vuole peggiorare ulteriormente questo problema, obbligando gli Internet provider e altre entità a registrare

le nostre comunicazioni, nel caso dovessimo essere soggetti a indagini in futuro. Tutto ciò non è soltanto pessima privacy e pessima sicurezza, è anche un duro colpo alle nostre libertà civili. Un mondo privo di conversazioni effimere è un mondo privo di libertà.

Non è possibile tornare indietro: le comunicazioni elettroniche sono una realtà che è destinata a durare. Ma dato che la tecnologia rende le nostre conversazioni meno effimere, occorrono delle leggi che possano frapporti e salvaguardare la privacy. È necessaria una legge sulla privacy delle informazioni il più possibile esaustiva, che protegga le nostre informazioni e comunicazioni a prescindere da dove vengano conservate o da come vengano elaborate. Occorrono leggi che costringano le aziende a mantenerle private e a distruggerle quando non servono più.

E dobbiamo ricordarci che, ogni qual volta scriviamo e inviamo qualcosa, siamo sotto osservazione.

Foley è un'anomalia. La maggior parte delle persone non invia messaggi istantanei per chiedere di fare sesso con minorenni. Le forze dell'ordine possono avere un'esigenza legittima di accedere ai messaggi istantanei, alle email e ai registri delle chiamate di Foley, ma è per questo motivo che esistono mandati suffragati da fondati elementi di prova: contribuiscono a garantire che le indagini si concentrino propriamente su sospetti pedofili, terroristi e altri criminali. Lo si è visto nei recenti arresti dei terroristi nel Regno Unito: sono state le indagini concentrate su sospetti terroristi a sventare il complotto, non la sorveglianza indiscriminata su vasta scala senza ragionevoli elementi di prova.

Senza legali protezioni della privacy, il mondo diventa un'enorme zona di sicurezza di un aeroporto, in cui il minimo scherzo (o commento fatto anni prima) può mettere una persona nei guai. Il mondo diviene così un gigantesco studio di ricerca di mercato, in cui tutti noi siamo dei soggetti per tutta la vita. Il mondo si converte in uno stato di polizia, in cui agli occhi del governo non siamo altro che dei Foley o dei terroristi.

Questo articolo è originariamente apparso su Forbes.com:

http://www.forbes.com/security/2006/10/18/nsa-im-foley-tech-security-cx_bs_1018security.html

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

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

Il profiling dei passeggeri delle linee aeree a scopo di lucro

Ho già scritto e parlato più volte in merito alle minacce per la privacy che scaturiscono dalla confluenza di interessi governativi e aziendali. A preoccuparmi non sono tanto le intenzionali invasioni della privacy da stato di polizia messe in atto dai governi, ma le invasioni della privacy di tipo commerciale da parte delle aziende, e come queste invasioni della privacy di stampo commerciale preparino il terreno per quelle governative e viceversa.

Il sistema di profiling dei passeggeri delle linee aeree preparato dal governo USA prese il nome di Secure Flight, e ne ho parlato diffusamente. A un certo punto il sistema avrebbe dovuto eseguire dei background check automatici su tutti i passeggeri, appoggiandosi a database governativi e commerciali (database di carte di credito, registri telefonici, qualsiasi cosa), e quindi assegnare a ogni persona un "valore di rischio" basato su quei dati. Gli individui con un alto

valore di rischio sarebbero stati controllati in maniera più approfondita rispetto a chi risultava avere un basso valore di rischio. È una totale perdita di tempo e un'enorme invasione della privacy, e l'ultima volta che sono andato a verificare avevano accantonato tutto questo.

Ma lo stesso identico sistema, totalmente inutile per individuare dei terroristi in un elenco di passeggeri, può rivelarsi eccellente per identificare i clienti. E quindi, ciò che il governo ha giustamente deciso di non fare risulta essere l'idea centrale della neonata impresa Jetera:

"Jetera inizierà con le informazioni che una compagnia aerea possiede sui vari passeggeri a bordo di un determinato volo, ottenendo dalle informazioni di prenotazione il nome, l'indirizzo, il numero di carta di credito e i punti fedeltà accumulati dal cliente. Tramite un procedimento (per il quale Jetera sta cercando un brevetto), l'impresa confronterà i dati di identificazione del passeggero con le montagne di informazioni sul suo conto disponibili presso uno dei tanti mastodontici istituti di credito, che mantengono sia informazioni di marketing che informazioni finanziarie, gestite separatamente. Jetera si collegherà al lato marketing, mostrando statistiche demografiche sui clienti, acquisti, interessi, atteggiamenti e simili.

"La manipolazione dei dati da parte di Jetera servirà a personalizzare l'intrattenimento a disposizione di ogni passeggero durante il volo. A un passeggero che risulta iscritto a una rivista di fai-da-te potrà essere offerto un video sulla lavorazione del legno. I registri degli acquisti per corrispondenza serviranno a evidenziare alcune offerte e a dare meno importanza ad altre. Gli appassionati di sport (individuabili attraverso i loro abbonamenti, gli acquisti di biglietti effettuati con carta di credito, iscrizioni a circoli sportivi, ecc.) potranno guardarsi 'Il Migliore' invece di 'Pretty Woman'".

L'articolo è datato 21 agosto 2006 ed è visibile solo agli abbonati. In gran parte tratta del potenziale di ricavo che offre il modello, dei finanziamenti ricevuti dalla compagnia, e degli incontri che ha avuto con anonime compagnie aeree. Nessuna compagnia aerea ha ancora accettato di ricevere il servizio, che non si limita alla personalizzazione delle offerte durante il volo, ma comprende anche pubblicità per corrispondenza pre- e post-volo e altri servizi ad hoc. Si parla della privacy a fine articolo:

"Jetera vede due questioni di ordine legale in merito alla privacy, e le risolve entrambe a suo favore. Nulla di quel che Jetera intende fare violerà la legge federale o le policy di privacy delle linee aeree così come vengono espresse sui loro siti Web. Per quanto concerne la percezione del cliente, Jetera non intende abusare la privacy di nessuno e offrirà l'opportunità di recedere dal servizio quando i passeggeri dovranno effettuare delle scelte sul tipo di intrattenimento che vorranno durante il volo.

"Se una compagnia aerea desidera abilitare la possibilità di recedere dal servizio in un altro punto del processo, Jetera farà il possibile per offrire tale possibilità, ha dichiarato McChesney. La privacy e il servizio al cliente verranno trattati in maniera specifica a ogni compagnia aerea, e Jetera si adeguerà a seconda di ognuna."

Il governo degli Stati Uniti già raccoglie informazioni personali dalle compagnie telefoniche, dagli alberghi e dalle società di autonoleggio, e dalle compagnie aeree. Quanto aspetterà prima di attaccarsi anche a questo sistema?

Anche l'altra faccia di tutto questo è fra le notizie: database commerciali che utilizzano informazioni governative:

"I registri che una volta le forze dell'ordine, i tribunali e gli istituti di correzione conservavano solo in formato cartaceo, vengono ora periodicamente digitalizzati e venduti in blocco al settore privato. Alcuni database commerciali oggi contengono più di 100 milioni di fedine penali. Vengono aggiornati con frequenza irregolare e fedine già cancellate ora spesso ricompaiono nel corso di accertamenti richiesti da datori di lavoro e padroni di casa".

http://www.aviationnow.com/search/AvnowSearchResult.do?reference=xml/awst_xml/2006/08/21/AW_08_21_2006_P55-56-01.xml&query=jetera oppure
<http://tinyurl.com/tt59x>
<http://www.nytimes.com/2006/10/17/us/17expunge.html>

I miei interventi precedenti sull'argomento:

http://www.schneier.com/blog/archives/2006/03/the_future_of_p.html
http://www.schneier.com/blog/archives/2005/09/secure_flight_n_1.html

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

Le news di Counterpane

BT acquisisce Counterpane:

Il 25 ottobre, British Telecom ha annunciato l'acquisizione di Counterpane Internet Security, Inc.

È un progetto a cui ho lavorato per circa un anno, e sono molto contento che si sia concretizzato.

<http://www.btplc.com/News/Articles/Showarticle.cfm?ArticleID=386c1b2f-0860-4afc-8f4a-26a066c12d10> oppure <http://tinyurl.com/yzmtn3>

I quotidiani:

http://today.reuters.com/news/articleinvesting.aspx?view=CN&storyID=2006-10-25T071554Z_01_L25202546_RTRIDST_0_TELECOMS-COUNTERPANE-BT-UPDATE-1.XML&rpc=66&type=qcna oppure <http://tinyurl.com/y28vr3>
<http://news.bbc.co.uk/1/hi/business/6083818.stm>
<http://www.businessweek.com/ap/financialnews/D8KVRV601.htm> oppure
<http://tinyurl.com/ylmw5f>
<http://business.timesonline.co.uk/article/0,,13129-2422003,00.html>
<http://business.guardian.co.uk/story/0,,1930942,00.html>
http://www.iht.com/articles/ap/2006/10/25/business/EU_FIN_COM_Britain_B_T_Group.php oppure <http://tinyurl.com/vxhvp>
<http://www.mercurynews.com/mld/mercurynews/business/technology/15847133.htm> oppure <http://tinyurl.com/wba9a>
<http://www.smh.com.au/news/TECHNOLOGY/BT-buys-security-specialist-Counterpane-cofounded-by-cryptologistSchneier/2006/10/26/1161749214324.html> oppure <http://tinyurl.com/y8632k>
<http://www.twincities.com/mld/twincities/15848925.htm>

Notizie da fonti del settore:

http://news.com.com/BT+snaps+up+Counterpane+Internet+Security/2100-1002_3-6129284.html oppure <http://tinyurl.com/y5hzeh>
http://news.zdnet.com/2100-1009_22-6129284.html
<http://www.redherring.com/Article.aspx?a=19374&hed=BT+Snags+Counterpane§or=Industries&subsector=Communications> oppure
<http://tinyurl.com/yxx6ej>
<http://www.scmagazine.com/uk/news/article/600346/bt-acquires-counterpan>

e-security/> oppure <http://tinyurl.com/v7rmh>
<<http://www.itweek.co.uk/vnunet/news/2167238/bt-buys-security-outsourcer>
> oppure <http://tinyurl.com/uq88x>
<<http://www.networkworld.com/news/2006/102506-bt-buys.html>
> oppure <http://www.techworld.com/security/news/index.cfm?newsID=7188&pagtype=al1>
> oppure <http://tinyurl.com/y7dzzf>
<<http://www.eetimes.com/news/latest/showArticle.jhtml?articleID=193402188>
> oppure <http://tinyurl.com/smvda>
<<http://www.ovum.com/news/euronews.asp?id=5014>
> oppure <http://news.moneycentral.msn.com/provider/providerarticle.asp?feed=OBR&Date=20061025&ID=6133629>
> oppure <http://tinyurl.com/y3lzaj>

La stampa estera:

<<http://www.theage.com.au/news/Technology/BT-buys-security-specialist-Counterpane-cofounded-by-cryptologistSchneier/2006/10/26/1161749214324.html>
> oppure <http://tinyurl.com/y36vt2>
<<http://press-releases.techwhack.com/5016/counterpane-bt/>
> oppure <http://www.metimes.com/storyview.php?StoryID=20061025-074107-7311r>
<<http://www.canada.com/topics/technology/news/gizmos/story.html?id=a177c27c-b5c6-4eb9-be30-a96cf83b8ed0&k=50643>
> oppure <http://tinyurl.com/y4wal4>
<<http://www.breakingnews.ie/2006/10/25/story282489.html>
> oppure <http://www.euro2day.gr/articlesfna/22917952/>
> oppure <http://www.net-security.org/secworld.php?id=4334>

I tabloid inglesi:

<<http://www.thesun.co.uk/article/0,,11039-2006490511,00.html>
> oppure http://www.mirror.co.uk/news/tm_headline=bt-in-code-war-&method=full&objectid=17992435&siteid=94762-name_page.html
> oppure <http://tinyurl.com/y2aqxy>

Il commento più bello che sia mai apparso sul mio blog:

<http://www.schneier.com/blog/archives/2006/10/bt_acquires_cou.html#c121821
> oppure <http://tinyurl.com/ug2oo>

Il commento di uno dei nostri investitori:

<<http://whohastimeforthis.blogspot.com/2006/11/british-telecom-dials-up-da-vinci-code.html>
> oppure <http://tinyurl.com/y6rdm3>

Il post sul mio blog:

<http://www.schneier.com/blog/archives/2006/10/bt_acquires_cou.html>

** **

Architettura e sicurezza

Li avrete visti di sicuro: quei grandi blocchi di cemento davanti a grattacieli, monumenti ed edifici governativi, ideati come protezione da auto e furgoni imbottiti di esplosivo. Sono spuntati come funghi nei mesi successivi all'11 settembre, ma l'idea di base è molto più antica. I più belli sono stati utilizzati anche come fioriere, i più brutti sono semplicemente rimasti al loro posto.

La forma segue la funzione. Dai castelli medievali ai moderni aeroporti, le preoccupazioni legate alla sicurezza hanno sempre influenzato l'architettura. I castelli apparvero durante il regno di Stefano di Inghilterra perché erano il sistema migliore per difendere il territorio e non vi era un re forte che ponesse limiti alla costruzione dei castelli. Ma la progettazione dei castelli è andata cambiando durante i secoli, in risposta a innovazioni belliche e politiche, dal tipo "motte-and-bailey" (traducibile in "terrapieno circolare con recinto")

al disegno concentrico nel periodo tardomedievale, fino ad arrivare a castelli unicamente decorativi nel XIX secolo.

Questi cambiamenti erano costosi. Il problema è che l'architettura aspira alla permanenza, mentre le minacce di sicurezza cambiano molto più velocemente. Una soluzione apparentemente buona nel periodo in cui un edificio venne progettato può non avere molto senso un secolo dopo (o anche una decina d'anni dopo). Ma a quel punto diventa molto difficile annullare tali decisioni architettoniche.

Quando la Syracuse University costruì un nuovo campus nella metà degli anni Settanta, le proteste studentesche dei tardi anni Sessanta erano ancora vive nella mente di ognuno. Pertanto gli architetti progettaronò un college privo degli spazi verdi tipici dei campus dei college. Ora sono passati trent'anni, ma la Syracuse University rimane immutata a difendersi contro una minaccia obsoleta.

Analogamente, negli anni Settanta gli ingressi degli alberghi a Montreal furono alzati rispetto al livello stradale, in risposta a preoccupazioni di sicurezza legate ai separatisti del Bloc Québécois. Oggi tale minaccia è scomparsa, ma rimane difficoltoso in modo esasperante accedere a quei vecchi alberghi.

Sempre negli anni Settanta, il consolato israeliano a New York costruì un sistema di sicurezza unico nel suo genere: un'entrata con doppie porte che consentiva alle guardie di identificare i visitatori e di controllare l'accesso all'edificio. Oggi questo tipo di ingresso è diffusissimo, e gli edifici che ne sono dotati continuano ad avere un aspetto scostante e inospitale anche molto tempo dopo la scomparsa della minaccia.

Lo stesso fenomeno si può notare anche nel cyberspazio. Nel suo libro "Code and Other Laws of Cyberspace", Lawrence Lessig parla di come le decisioni in merito alla infrastruttura tecnologica (l'architettura di internet) si incorporano e diventano impossibili da cambiare. Che si tratti di tecnologie per la prevenzione della copia di file, per limitare l'anonimato, per registrare le nostre abitudini digitali per una indagine successiva, o per ridurre l'interoperabilità e rafforzare posizioni monopolistiche, una volta che le tecnologie basate su queste problematiche di sicurezza si standardizzano, ci vogliono decenni prima di poterle smantellare.

È pericolosamente miope prendere decisioni architettoniche basate sulla minaccia del momento senza tenere in considerazione le conseguenze a lungo termine di tali decisioni.

Le barriere di cemento degli edifici fanno eccezione: si possono togliere. Sono apparse per la prima volta a Washington DC nel 1983, dopo il camion bomba che colpì gli accampamenti militari dei Marines a Beirut. Dopo l'11 settembre erano considerati una specie di bizzarro status symbol: erano la prova che un determinato edificio fosse abbastanza importante da meritare protezione. Solo nella città di New York più di 50 palazzi vennero protetti in questo modo.

Oggi vengono lentamente smantellate. Degli studi hanno dimostrato che intralciano il traffico, che diventano degli enormi posacenere e che possono rappresentare un rischio di sicurezza diventando schegge pericolosissime se fatte esplodere.

Dobbiamo essere grati del fatto che possano essere rimosse, e che non siano diventate tratti permanenti dell'architettura delle nostre città. Non saremo così fortunati per quanto riguarda alcune delle attuali decisioni progettuali sull'architettura di internet.

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

Fermate la mia auto, per favore

I residenti di Prescott Valley sono invitati a registrare la propria auto nel caso non guidino a notte fonda. La polizia fermerà quelle auto nel caso si trovino per strada in quell'intervallo di tempo, assumendo che siano rubate:

"Watch Your Car è un programma volontario in cui i possessori di un veicolo lo immatricolano all'AATA. Il veicolo viene quindi inserito in un database speciale, sviluppato e mantenuto dall'AATA, il quale è direttamente collegato alla MVD, Motor Vehicle Division.

"I partecipanti poi applicano sul parabrezza e sul lunotto gli adesivi Watch Your Car. Così facendo, i proprietari dei veicoli segnalano agli agenti delle forze dell'ordine che il proprio mezzo non viene abitualmente utilizzato fra la una e le cinque del mattino, il periodo in cui avviene la maggior parte dei furti.

"Se un agente di polizia nota uno di questi veicoli circolare in questa fascia oraria, ha il permesso di farlo accostare e di interrogare il conducente. Mediante l'accesso al database MVD, l'agente potrà stabilire se il veicolo è stato rubato o meno. Il programma inoltre consente agli agenti delle forze dell'ordine di informare il proprietario del mezzo immediatamente dopo l'accertamento dell'utilizzo illegale del veicolo".

Questo programma è interamente facoltativo, ma presenta una grave esternalità. Se la polizia perde tempo a inseguire falsi allarmi, non può intervenire in altre situazioni. Se la città facesse pagare ai proprietari delle auto una multa per ogni falso allarme, non avrei nulla da eccepire su questo programma. Non deve essere necessariamente una multa elevata, ma sufficiente a compensare i costi per la città. Non è per nulla diverso da quei dipartimenti di polizia che multano i proprietari di casa per falsi allarmi antifurto nei casi in cui i sistemi di allarme sono collegati direttamente con le centrali di polizia.

<http://www.pvaz.net/Services/police/watchyourcar.htm>

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

La sicurezza della merce imbarcata sugli aerei

La BBC ha riportato una "considerevole" breccia nella sicurezza della merce imbarcata per via aerea. Sostanzialmente, le merci vengono caricate su voli passeggeri senza essere controllate. Un sedicente terrorista potrebbe quindi far saltare un aereo passeggeri inviando una bomba tramite FedEx.

In generale, le merci non necessitano tutti quei controlli di sicurezza che vengono effettuati sui passeggeri. Il ragionamento è il seguente: gli aerei per trasporto merci rappresentano un rischio terroristico molto minore rispetto agli aerei passeggeri, perché lo scopo del terrorismo è provocare la morte di persone innocenti. Far saltare un aereo carico di pacchi della FedEx è seccante, ma non provoca terrore quanto l'esplosione di un aereo carico di turisti. Pertanto, non è necessario che la sicurezza intorno alle merci sia eccessivamente rigorosa.

Detto questo, se la maggior parte delle merci spedite per via aerea viaggiano su aerei per il trasporto merci, allora può essere ragionevole far viaggiare una piccola quantità di carico (assumendo che venga scelta casualmente e che lo spedizioniere non conosca già il contenuto dei vari pacchi) come bagaglio sugli aerei passeggeri. Un sedicente terrorista farebbe meglio a prendere il suo ordigno e a far esplodere un autobus che non a spedirlo nella speranza che sia imbarcato su un aereo passeggeri.

Almeno, questa è la teoria. Ma teoria e pratica sono due cose diverse.

Il sistema inglese prevede i cosiddetti "known shipper" (lett. spedizionieri conosciuti):

"Grazie a un sistema chiamato 'known shipper' o 'known consignor', quelle aziende che sono state controllate accuratamente da agenti di sicurezza incaricati dal governo possono inviare pacchi per via aerea senza venire sottoposti a ulteriori controlli di sicurezza.

"A meno che un pacco di un known shipper susciti sospetti o venga sottoposto a controlli casuali, ci si fida ciecamente della sicurezza del contenuto".

Ma:

"Il capitano Gary Boettcher, presidente della US Coalition Of Airline Pilots Associations, sostiene che il sistema 'known shipper' è 'probabilmente il punto più debole della sicurezza delle merci oggi'.

"Negli Stati Uniti vi sono circa un milione e mezzo di known shipper. Vi sono migliaia di spedizionieri merci. In qualsiasi punto del percorso i pacchi possono essere intercettati in mano a queste organizzazioni", ha affermato.

"Anche quelle compagnie rispettabili e affidabili non fanno in realtà chi si trova in magazzino, chi sta armeggiando con i pacchi, chi li sta assemblando".

Questo sistema è già stato sfruttato dai trafficanti di droga:

"Il signor Adeyemi ha introdotto chili di cocaina in Inghilterra in qualità di carico spedito per via aerea senza alcun controllo, e trasportato dagli Stati Uniti dalla compagnia di spedizioni Federal Express. Non ha nemmeno dovuto pagare le spese postali.

"Ciò è stato possibile perché Adeyemi è riuscito a comprare illegalmente da un ex dipendente i numeri di conto FedEx confidenziali di aziende rispettabili e autorizzate.

"Un suo complice negli Stati Uniti è riuscito a mettere i numeri di conto sui pacchi di droga i quali, dato che sembravano essere stati inviati da spedizionieri conosciuti, sono arrivati senza alcun controllo all'aeroporto di Stansted.

"Quando la polizia ha poi contattato le aziende i cui conti e le cui autorizzazioni erano stati abusati a tal punto, si è scoperto che quelle compagnie non avevano avuto il benché minimo sospetto in merito all'irregolarità".

E non è così sicuro che un terrorista non possa scoprire quali carichi hanno maggiori probabilità di essere imbarcati su aerei passeggeri:

"Tuttavia, molte grandi aziende come FedEx e UPS mettono a disposizione

dei clienti la possibilità di seguire online lo stato della spedizione.

"Si tratta di una funzionalità che, secondo Chris Yates, esperto di sicurezza aerea della Jane's Transport, potrebbe essere sfruttata dai terroristi.

"Nel caso si cerchi di far arrivare della merce da Heathrow a New York a una certa ora del giorno, dai tracciati online si può ottenere una stima abbastanza precisa di quando un determinato pacco si troverà in volo".

E secondo la BBC il 70% delle merci viene spedito mediante aerei passeggeri. Sembra una cifra un po' troppo alta.

Se avessimo un budget illimitato, potremmo controllare tutte le merci senza problemi. Ma non abbiamo una tale quantità di denaro, e ignorare gli aerei per il trasporto merci per concentrarsi sugli aerei passeggeri è un compromesso di sicurezza ragionevole. Ma vi sono delle falle tremendamente grandi in questo sistema.

<http://news.bbc.co.uk/2/hi/americas/6059742.stm>

** *** *****

Cheyenne Mountain va in pensione

Cheyenne Mountain è stato per lungo tempo il posto di comando sotterraneo degli Stati Uniti, progettato per resistere a un colpo diretto di una testata nucleare. Costruito negli anni Sessanta, è una reliquia che risale alla Guerra Fredda, e chiudere il sito è probabilmente una buona idea. Ma questo paragrafo mi fa esitare:

"Keating ha dichiarato che il nuovo centro di comando, al contrario, potrebbe essere danneggiato nel caso un terrorista pilotasse un jumbo jet e in qualche modo sapesse esattamente dove schiantarlo. Ma 'è molto improbabile che ciò accada', ha affermato Keating".

Certo, è un bersaglio terroristico piuttosto improbabile, però...

<http://apnews.myway.com/article/20061016/D8KPU1C02.html>

** *** *****

Commenti dei lettori

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

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

** *** *****

CRYPTO-GRAM è una newsletter mensile gratuita che offre riassunti, analisi, approfondimenti, e commenti sulla sicurezza (informatica e in generale) e sulla crittografia. I numeri arretrati sono disponibili all'indirizzo <http://www.schneier.com/crypto-gram.html>. Per iscriversi, cancellare l'iscrizione o cambiare il proprio indirizzo a

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

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

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

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

Per informazioni <crypto-gram@communicationvalley.it>

I commenti a CRYPTO-GRAM devono essere inviati a
schneier@counterpane.com. Si sottintende il permesso di riprodurre tali
commenti, salvo indicazione contraria. I commenti possono venire
adattati per ragioni di spazio e di chiarezza.

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

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

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. 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 Counterpane Internet Security, Inc.

Copyright (c) 2006 - Bruce Schneier.