



È interessante a questo punto fare delle ipotesi su chi possa utilizzare il codice. Ovviamente in capo alla lista ci sono gli hacker, che potrebbero esaminarlo alla ricerca di vulnerabilità da sfruttare. Questi potrebbero essere hacker che agiscono in proprio, o alle dipendenze degli spammer, oppure anche come parte del crimine organizzato. Credo che cose del genere potranno accadere, ma non in misura rilevante. Le vulnerabilità di Microsoft non sono difficili da trovare, e la gente non ha così disperatamente bisogno del codice sorgente per trovarle.

Un altro gruppo che potrebbe essere interessato al codice è rappresentato dalle aziende che scrivono software compatibile. Ma dubito che vi sia qualcosa di utile per loro. Non varrebbe il denaro speso per far esaminare il codice a un team di programmatori, alla ricerca di chiamate di sistema nascoste e trucchi di programmazione, soprattutto perché nulla garantisce che quei trucchi funzioneranno ancora con la prossima revisione del software.

Un terzo gruppo potrebbero essere degli avvocati in cerca di azioni legali. È da molto tempo che si dice che Windows contenga delle scorciatoie accessibili soltanto dal software Microsoft e non dai prodotti della concorrenza. Potrebbe valere la pena, per un avvocato, ingaggiare un team di programmatori in modo che trovino delle prove inconfutabili; prove, ad esempio, dell'esistenza di codice che faciliti Microsoft Office e blocchi StarOffice. Ma anche in questo caso, ritengo si tratti di qualcosa di troppo rischioso da portare avanti.

Le organizzazioni di intelligence nazionale sono un possibile quarto gruppo interessato al codice. Può essere, ma credo che qualsiasi organizzazione di intelligence che si rispetti, interessata a una copia del codice, sia già in possesso di quella copia.

La reazione di Microsoft dimostra come anch'essa abbia fatto questi ragionamenti. Secondo un articolo di Information Week "Lo scorso mercoledì Microsoft ha dichiarato che sono state inviate delle comunicazioni di avviso a tutti coloro che hanno illegalmente scaricato il codice sorgente di Windows". Se solo consideriamo la minaccia rappresentata dagli hacker, questa di Microsoft è una mossa straordinariamente stupida. Il codice è già fuori. È di dominio pubblico. Non si può ritirarlo. Qualunque malintenzionato interessato al codice ora ce l'ha, e non si farà certo intimidire dalla lettera di un avvocato. L'unica cosa che stanno facendo ora i legali di Microsoft è impedire ai "buoni" di esaminare il codice, ed eventualmente di trovare delle vulnerabilità che Microsoft potrebbe poi sistemare.

Ma se teniamo presente che la paura più grande di Microsoft è rappresentata forse da altri avvocati, allora quella mossa ha senso. Microsoft vuole limitare il numero di brave persone che abbiano accesso al codice, perché teme quel che potrebbero trovare.

Una qualsiasi azienda che avesse a cuore la sicurezza dei dati risponderebbe ammettendo l'errore e cercando di riparare la falla di sicurezza che ha causato la diffusione non autorizzata del codice, e infine esaminando essa stessa il codice ormai pubblico per sistemare celermente quanti più bug possibili. Inoltre si renderebbe conto che gli hacker sono in possesso del codice e potrebbero servirsene, e non impedirebbe ai benintenzionati di difendersi.

Ritengo che in questo modo Microsoft avrebbe potuto fare una miglior figura a livello di pubbliche relazioni, invece di far subentrare gli avvocati.

<<http://www.informationweek.com/story/showArticle.jhtml?articleID=17701340>> oppure <<http://tinyurl.com/3a2w3>>  
<[http://www.winnetmag.com/windowspaulthurrott/Article/ArticleID/41788/windowspaulthurrott\\_41788.html](http://www.winnetmag.com/windowspaulthurrott/Article/ArticleID/41788/windowspaulthurrott_41788.html)> oppure <<http://tinyurl.com/26kca>>  
<<http://www.cnn.com/2004/TECH/internet/02/13/microsoft.code.ap/>>  
<[http://news.com.com/2100-7349\\_3-5158496.html](http://news.com.com/2100-7349_3-5158496.html)>

Il rapporto secondo cui Microsoft è l'origine della fuga di notizie:

<<http://www.eweek.com/article2/0,4149,1526831,00.asp>>

\*\* \*\*

## Un virus di ingegneria sociale

Alcuni anni fa ho parlato dell'aumento degli attacchi semantici: attacchi informatici che hanno come bersaglio l'utente piuttosto che errori di interpretazione del software. Un ovvio esempio è dato dalle e-mail truffaldine che cercano di invitare l'utente a fare clic sull'allegato. Ormai sono in circolazione da diverso tempo, e continuano a migliorare. Questa è una che ho ricevuto di recente (l'allegato contiene il virus Bagle.J). Anche se presenta qualche errore grammaticale, che sembra essere distintivo di questo tipo di comunicazioni (ci sarà qualche propagatore di virus in grado di scrivere in inglese?), è tutto molto convincente:

Caro utente, la direzione del mailing system NOMEDOMINIO.COM intende farle sapere che alcuni dei nostri clienti hanno espresso lamentele in merito allo spam (posta indesiderata) proveniente dal suo account e-mail. È probabile che lei sia stato infettato da un virus Trojan che fa da proxy-relay server. Per mantenere sicuro il suo computer, la preghiamo di seguire le istruzioni e di leggere l'allegato per maggiori dettagli.

Il file allegato è protetto da password per ragioni di sicurezza. La password è 64003.

La Direzione,

team NOMEDOMINIO.COM

<http://www.NOMEDOMINIO.COM>

[Allegato chiamato "message.zip"]

Il mio articolo sugli attacchi semantici:

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

\*\* \*\*

## News

Un articolo davvero buono sulla matematica che sta dietro a Rijndael, l'Advanced Encryption Standard (AES).

<<http://research.sun.com/people/slandau/maa1.pdf>>

Ecco un'ovvia variazione alla serie "I cattivi introducono di nascosto una bomba su un aereo". Qui i cattivi fanno entrare l'ordigno diviso in parti, una alla volta, passando attraverso la sicurezza, e poi lo montano a bordo. Mi fa venire in mente quel gruppo del MIT che era riuscito a vincere milioni di dollari ai casinò tenendo il conto delle carte a blackjack. I casinò sapevano come individuare i "contacarte", ma il gruppo aveva diviso i compiti fra varie persone, in modo che ognuna di esse, presa singolarmente, non destasse sospetti. Questa tattica di distribuzione di un attacco funziona in diversi settori della sicurezza, e può essere molto difficile da contrastare.

<<http://observer.guardian.co.uk/international/story/0,6903,1143524,00.html>>

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

Honeypot nelle reti wireless.

<<http://www.securityfocus.com/infocus/1761>>

È disponibile il codice di exploit per una recente vulnerabilità di ASN.1:

<[http://searchsecurity.techtarget.com/originalContent/0,289142,sid14\\_gci950665,00.html](http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci950665,00.html)> oppure <<http://tinyurl.com/2ssku>>

Ben Cohen, della società Ben & Jerry's Ice Cream ha lanciato la campagna "The Computer Ate My Vote" (Il computer si è mangiato il mio voto), per far pressione affinché venga implementata una maggiore sicurezza nelle macchine per il voto elettronico.

<<http://www.wired.com/news/business/0,1367,62294,00.html>>

La polizia tedesca sta utilizzando gli SMS per diffondere informazioni in merito a persone scomparse e ai latitanti. Presumibilmente il prossimo passo saranno le immagini.

<<http://www.siliconvalley.com/mld/siliconvalley/news/7965775.htm>>

Esistono ora dei tool automatizzati per effettuare hack di Bluetooth. Ciò significa che verranno sfruttati da persone sempre meno in gamba e senza scrupoli.

<<http://www.silicon.com/networks/mobile/0,39024665,39118440,00.htm>>

Un articolo di opinione sull'inutilità delle leggi anti-spam:

<<http://www.silicon.com/research/specialreports/protectingid/0,3800002220,39118479,00.htm>> oppure <<http://tinyurl.com/37ccq>>

Intanto AOL, EarthLink, Microsoft e Yahoo hanno separatamente intentato cause contro gli spammer negli Stati Uniti, rifacendosi alla legge CAN-SPAM. Stanno lavorando insieme per rafforzare la loro posizione:

<<http://www.internetretailer.com/dailyNews.asp?id=11500>>

<[http://seattlepi.nwsourc.com/business/127114\\_spam18.html](http://seattlepi.nwsourc.com/business/127114_spam18.html)>

<<http://www.pcworld.com/news/article/0%2Caid%2C112212%2Cpg%2C1%2C00.asp>> oppure <<http://tinyurl.com/2t63a>>

Una società dell'industria cinematografica ha denunciato un'azienda che vende software per copiare DVD:

<<http://www.siliconvalley.com/mld/siliconvalley/news/editorial/7950558.htm>>

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

<<http://news.zdnet.co.uk/business/legal/0,39020651,39146323,00.htm>>

<[http://www.usatoday.com/tech/world/2004-02-16-canada-music-swamps\\_x.htm](http://www.usatoday.com/tech/world/2004-02-16-canada-music-swamps_x.htm)> oppure <<http://tinyurl.com/23lj5>>

Triste vicenda sulle conseguenze di un furto d'identità.

<<http://msnbc.msn.com/id/4264051/>>

Truffa "low-tech" ai danni delle carte di credito. Il personale di servizio di un ristorante copia i numeri di carta di credito dei clienti e li passa a terzi, che poi realizzano carte di credito fasulle.

<<http://www.mercurynews.com/mld/mercurynews/news/local/7988627.htm>>

La corte ha stabilito che JetBlue non ha violato alcuna legge quando ha fornito informazioni sui passeggeri a fornitori della difesa degli Stati Uniti. Ciò non mi sorprende. Si è trattato certamente di una violazione di fiducia, non delle leggi.

<[http://www.usatoday.com/tech/news/techpolicy/2004-02-20-jetblue-privacy\\_x.htm](http://www.usatoday.com/tech/news/techpolicy/2004-02-20-jetblue-privacy_x.htm)> oppure <<http://tinyurl.com/35axx>>

"Se centinaia di migliaia di persone continuano imperterrite a fare clic su qualsiasi allegato si trovano nella loro casella di posta elettronica, c'è qualche speranza di attenuare la minaccia rappresentata da centinaia di migliaia di sistemi compromessi con backdoor aperte?"

<<http://www.securityfocus.com/columnists/221>>

Un'ennesima prova di come la tecnologia abbia reso le fotografie un mezzo inaffidabile per dimostrare il vero. Qualcuno ha modificato una foto di John Kerry che lo ritrae ad una

manifestazione contro la guerra, e ci ha aggiunto Jane Fonda.

<<http://sfgate.com/cgi-bin/article.cgi?f=/c/a/2004/02/20/MNG4S54RGO1.DTL>>

oppure <<http://tinyurl.com/2p9vp>>

Il programma Protected Critical Infrastructure Information (PCII) del Dipartimento della Sicurezza Nazionale è fonte di problemi di sicurezza. Permettendo alle aziende di inviare i dettagli sulle vulnerabilità di sicurezza e tenendo l'opinione pubblica all'oscuro di queste informazioni, è qualcosa che può essere usato per nascondere eventuali negligenze o comportamenti criminali.

<<http://www.securityfocus.com/news/8090>>

Un'altra idea per mantenere la privacy navigando nel Web:

<[http://zdnet.com.com/2100-1104\\_2-5164413.html](http://zdnet.com.com/2100-1104_2-5164413.html)>

C'è un nuovo gruppo di aziende negli Stati Uniti: undici compagnie di sicurezza hanno formato la Cyber Security Industry Alliance (CSIA).

<<http://www.washingtonpost.com/wp-dyn/articles/A3455-2004Feb24.html>>

Applicare patch è ancora troppo difficile e troppi amministratori di reti continuano a non farlo.

<<http://news.zdnet.co.uk/internet/security/0,39020375,39147340,00.htm>>

La paura del cyber-terrorismo continua ad essere alimentata:

<<http://www.latimes.com/technology/la-na-cyber24feb25,1,7457295.story>>

Rischi nell'utilizzo delle reti presenti negli alberghi:

<<http://edition.cnn.com/2004/TRAVEL/02/25/biz.trav.security>>

Serie di utility freeware Windows per il recupero delle password:

<<http://freehost14.websamba.com/nirsoft/utills/index.html>>

Un'interessante ricerca sui sistemi IDS:

<[http://www.gcn.com/vol1\\_no1/daily-updates/25155-1.html](http://www.gcn.com/vol1_no1/daily-updates/25155-1.html)>

Un altro intervento nel dibattito su sicurezza open-source contro sicurezza closed-source:

<<http://www.theregister.co.uk/content/55/36029.html>>

Alcune aziende stanno cercando di ridurre le proprie responsabilità nel caso che le vostre informazioni personali venissero rubate.

<<http://www.washingtonpost.com/wp-dyn/articles/A31874-2004Mar4.html?referrer%3Demail>> oppure <<http://tinyurl.com/2rbuc>>

Come le forze dell'ordine sono riuscite ad intercettare i telefoni cellulari anonimi dei terroristi:

<<http://www.iht.com/articles/508783.html>>

<<http://www.theregister.co.uk/content/28/36060.html>>

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

Le News di Counterpane

NOVITÀ: Crypto-Gram è ora disponibile anche in formato RSS:

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

Chiunque abbia difficoltà a ricevere Crypto-Gram a causa dei filtri antispam può tenere in considerazione questa opzione.









costruisce una serie di domande a cui solo voi potete rispondere. "Quale fra queste cinque banche vi ha concesso un prestito?", "A quale dei seguenti indirizzi abitavate prima?". Dovete fare richiesta di persona, e rispondere a queste domande inserendo le risposte in un computer e di fronte a un funzionario. Se siete in grado di rispondere alle domande, il sistema dà per assodato che voi non siete un impostore.

Ammettendo che tutte le verifiche abbiano successo, il funzionario registra un certo numero di impronte digitali della persona e rilascia una tessera V-ID. Questa scheda contiene informazioni relative alla persona; magari una fotografia; forse le informazioni sulle impronte digitali e di certo un numero di identificazione.

(Presumibilmente, il sistema del documento d'identità aziendale è analogo, con qualche requisito in più deciso dall'azienda -- che stabilisce chi avrà la tessera -- e la presenza del logo aziendale sulla tessera. Ma le tessere aziendali potranno essere utilizzate nel sistema generale, e Brill ritiene che sarà questo a dare un grande impulso al sistema. Non sono sicuro, però, su quel che potrebbe accadere quando un individuo presente sul libro paga di una ditta si scopre essere su una watch list di sospetti terroristi. Probabilmente la tessera fungerà da documento d'identità aziendale, e non nazionale).

I punti di controllo di sicurezza che accettano la tessera dovranno essere dotati di un qualche dispositivo di lettura. Questo dispositivo potrebbe contenere o meno l'intero database delle impronte digitali. L'elenco di tessere valide sarà sicuramente aggiornato quotidianamente, per tener traccia di chi entra e di chi esce dalle varie watch list governative. Il dispositivo avrà un lettore di impronte digitali e una fessura per la tessera, e un qualche tipo di indicatore visivo che faccia sapere al personale di sicurezza che il possessore della tessera è in regola.

La tessera sarà multiuso. Brill immagina che aeroporti, edifici governativi, stadi, monumenti nazionali, palazzi di uffici effettueranno controlli su chi entra. Chi avrà la tessera potrà entrare in una sorta di corsia preferenziale, dove effettuerà il controllo delle impronte digitali e attraversare le misure di sicurezza con meno impicci. Chi non avrà la tessera, dovrà mettersi nella corsia dei "non verificati" e presumibilmente subirà una serie di controlli più minuziosi.

Questo è come dovrebbe funzionare il sistema. Ora vediamo in che misura potrebbe realmente funzionare.

Il sistema non è stato ancora progettato completamente, ma pare che le impronte digitali verranno usate per autenticare il possessore della tessera, e non per identificarlo. Questa è una buona cosa. Presumo poi che i dati presenti sulla carta saranno ben protetti. Naturalmente vi sono molti modi per ingannare i lettori di impronte digitali, ma avere una guardia che osserva l'individuo mettere il proprio dito sul lettore è il miglior modo per garantirne un uso appropriato. Le mie preoccupazioni non riguardano come il sistema viene utilizzato, ma hanno a che vedere con la registrazione e l'amministrazione del database back-end.

Sarebbe di certo possibile ottenere una tessera sotto falso nome, esattamente come lo è ottenere qualsiasi altro genere di documento identificativo (anche un passaporto) sotto falso nome. Se da un lato il sistema V-ID non emetterà deliberatamente delle tessere a chi non dovrebbe averle, dall'altro sarà progettato per far sì che non sia difficoltoso avere una tessera. Le domande Choicepoint sono un'idea arguta, ma il database è stato sviluppato per proteggersi da un genere ben diverso di aggressori. Bisognerà riflettere a lungo sul database Choicepoint e su quali contromisure mettere in atto in relazione a questo nuovo tipo di aggressore.

Le persone considerate fidate da Choicepoint e dalla V-ID costituiscono naturalmente un potenziale problema. Molti dei terroristi dell'11 settembre possedevano autentiche patenti di guida dello stato della Virginia sotto falso nome, patenti che sono state emesse da impiegati statali corrotti. Questo sistema non sarà immune dallo stesso tipo di problema, anche se immagino che chi l'ha ideato farà ogni sforzo possibile per ridurre i rischi.

È il sistema back-end che mi preoccupa. Da qualche parte ci sarà un computer che genera le domande, che confronta le informazioni di identità con i database del governo, e che amministra in generale l'intero sistema. Il database delle impronte digitali verrà memorizzato da qualche parte, possibilmente su ogni lettore. Questi database saranno vulnerabili agli attacchi, sia dall'interno che dall'esterno.

Una contro-argomentazione a questa analisi può essere che la maggior parte della gente non sarà in grado di sovvertire il sistema, sia sbaragliando la tessera, o il lettore di impronte digitali o il database back-end, oppure manipolando il sistema in modo che emetta una tessera con un falso nome. La maggioranza delle persone otterrà (o meno) una tessera onestamente, e userà il sistema correttamente e anche se alcuni saranno in grado di attaccare il sistema con successo, non è una ragione per bocciarlo in toto. Ma lo scopo primario di questo sistema è quello di funzionare anche di fronte a un avversario scrupoloso e tutt'altro che sprovveduto, ed è fuori luogo anche l'opinione secondo cui la maggior parte dei terroristi è gente stupida. Non importa se l'uomo medio possa o meno sovvertire il sistema: i sistemi di sicurezza ci devono proteggere contro persone intelligenti e in gamba, specialmente terroristi intelligenti e in gamba.

Il sistema è progettato per essere decentralizzato, così che nessuno possa essere rintracciato quando si serve della tessera. È una questione aperta se le forze dell'ordine potranno obbligare o meno l'azienda a cambiare questo aspetto e ad usare il sistema per rintracciare le persone. L'infrastruttura è già in grado di farlo: abbiamo un software sul lettore e un sistema di comunicazione che collega i lettori ad un qualche nucleo centrale. Brill ha detto che sarà una cosa impossibile, ma dalla sua descrizione del sistema ciò è palesemente falso. Ha anche detto che una cosa simile non potrebbe mai accadere perché sarebbe una violazione del contratto che la compagnia V-ID ha stipulato con i propri clienti, ma a mio avviso questo non ha senso.

Le mie principali preoccupazioni riguardanti questo sistema nascono da ciò che sta cercando di fare. Nei suoi scritti e nei suoi discorsi, Brill è molto attento nello spiegare che queste non sono "documenti di viaggio certificati", ma "carte di identità verificate". Però l'unico obiettivo delle sue tessere è quello di dividere la gente in due file -- una corsia normale e una preferenziale, una corsia "da controllare di più" e una "da controllare di meno", o comunque vogliamo chiamarle (ogni punto di controllo di sicurezza che utilizza la tessera svilupperebbe le proprie procedure a riguardo). Questa divisione ha senso solamente se si basa su una condizione di fiducia. Se non credete che le persone dotate di tessera siano maggiormente fidate, non le farete passare dalla corsia preferenziale. Ecco un esempio: se io ideassi una tessera che certificasse l'igiene orale di una persona, voi non dividereste la gente in due file basandovi su quella tessera, perché sapete che le persone con una buona igiene orale non sono più fidate di coloro che non l'hanno. D'altra parte, sarebbe valido utilizzare quella tessera per dividere la gente in due file in uno studio dentistico, basandosi sul presupposto che le persone con una buona igiene orale verrebbero trattate più velocemente. Secondo il piano di Brill, i possessori di tessera riceveranno un controllo di sicurezza più blando rispetto a chi non la possiede. Possiamo girare intorno al concetto finché vogliamo, ma questo sta a significare che i possessori della tessera sono persone più fidate di chi non ce l'ha.

La realtà delle cose è che l'esistenza della tessera viene a creare una terza, pericolosissima, categoria: i malintenzionati in possesso della tessera. Timothy McVeigh sarebbe stato in grado di avere una di queste tessere. Il cecchino di Washington DC e Unabomber sarebbero stati in grado di avere questa tessera. Qualsiasi talpa che lavora per dei terroristi e che è tuttora incensurata sarebbe in grado di averla. Alcuni dei terroristi dell'11 settembre avrebbero potuto ottenere un documento del genere. Tutte queste sono persone che il sistema indicherebbe come degne di fiducia, quando non lo sono affatto.

Ancora peggio, il sistema permette ai terroristi di testarlo in anticipo. Immaginate di appartenere a un gruppo terroristico. Dodici di voi fanno richiesta per la tessera, ma solo quattro la ottengono. Questi quattro non solo possiedono un documento che permette loro di passare dai posti di controllo con più facilità, ma sanno anche di non risultare in nessuna watch list. Chi saranno i quattro designati per la prossima missione, secondo voi? Facendo in modo

che la fiducia venga "pre-concessa", si sta costruendo un sistema molto più facile da sbaragliare.

Inoltre, qualsiasi intrusione nel sistema è un problema ancor più grave, perché può avere le applicazioni più svariate. La letteratura dell'azienda considera un problema il fatto che "gli americani hanno ora bisogno di diverse tessere di identificazione/sicurezza", ma questa in effetti è una funzionalità di sicurezza. Se un terrorista sovverte il sistema V-ID, lo può sfruttare per penetrare impunemente in qualsiasi struttura che fa uso di quel sistema e questo è un grave punto debole. Confrontiamolo con il caso di un documento identificativo aziendale, che consente l'accesso solo alle strutture di una certa azienda: sovvertire questo sistema permetterebbe all'aggressore di penetrare solamente in quelle strutture, e nient'altro.

Tutto ciò fa emergere un'altra domanda fondamentale: perché i vari posti di controllo di sicurezza dovrebbero accettare una tessera V-ID? Questo sistema ha un costo non indifferente di installazione negli aeroporti, negli stadi, e così via. Tali strutture devono comprare i lettori di tessere, per cui deve esserci qualche beneficio in risposta. Il beneficio dichiarato è il servizio clienti: i possessori di tessera possono ricevere un trattamento migliore. Le compagnie aeree hanno da molto tempo compreso il problema di costringere i propri clienti migliori ad attendere in lunghissime code ai posti di controllo, ed hanno quindi implementato delle corsie preferenziali per i passeggeri di prima classe e per chi vola frequentemente. Ma per il proprietario di uno stadio, una persona con una tessera V-ID non è un cliente speciale, è solo uno che ha pagato per avere una tessera V-ID. Quale beneficio può derivare, per uno stadio, a dividere le persone su questa base? L'unico che mi viene in mente è la responsabilità: mediante il sistema V-ID lo stadio riceve una sorta di copertura in casi di responsabilità quando chi è in possesso di una tessera commette qualche infrazione.

Si tratta di una questione molto seria, e di estrema importanza per gli affari della Verified Identity Card, Inc. L'azienda vuole identificarsi in una carta d'identità volontaria nazionale ma allo stesso tempo non vuole essere considerata responsabile per esserlo, se mi consentite il gioco di parole. Ecco perché cercano in tutti i modi di non chiamare "fidati" i possessori di tessera. Ma perché un'azienda dovrebbe accettare la tessera se, nel caso qualcuno in possesso di tessera causasse problemi, l'azienda venisse considerata responsabile? L'azienda ha convalidato la tessera e il sistema che la supporta, affidandosi alla capacità del sistema nel distinguere chi è fidato da chi non lo è. Il motivo per cui le industrie accettano documenti identificativi emessi dal governo è che la corte lo considera una credenziale più che ragionevole. Il proprietario di un negozio di alcolici può difendersi in tribunale dicendo: "Lui aveva una patente di guida". Che cosa significherebbe in questo caso "lui aveva una tessera V-ID", visto che la compagnia V-ID si rifiuta di accettare ogni responsabilità?

Dal suo punto di vista, la V-ID è furba a non voler accettare di essere ritenuta responsabile. Ed ha perfettamente ragione nell'affermare che un possessore di tessera non è più fidato di chi non possiede quel documento, anche se affermando questo la compagnia espone la falla più evidente del proprio modello di business. Se l'amministrazione di un palazzo decide che tutte le persone dovranno passare attraverso un metal detector, non ha senso controllare solo chi non è in possesso di una tessera V-ID. Se un aeroporto intende implementare delle procedure extra di controllo su un ristretto numero di passeggeri, non ha senso basare tale decisione sul possesso o meno di una tessera V-ID. I terroristi possono avere mille volti, e l'ultima cosa che vogliamo è che un terrorista sia in possesso di una tessera V-ID che gli permetta di operare in totale impunità.

La sicurezza è sempre un bilanciamento, un compromesso. La domanda da farsi non è "Questo sistema ci rende più sicuri?", altrimenti tutti indosserebbero giubbetti antiproiettile e ci rinchiuderebbero nelle nostre case. La domanda da porsi è "Questo sistema vale i compromessi che comporta?" Il sistema V-ID comporta dei compromessi e dei bilanciamenti molto gravi. Il sistema raccoglie un database di impronte digitali di tutti coloro che fanno richiesta della tessera, un database che può venire usato e abusato da chiunque ne abbia accesso, legittimo o illegittimo.





Anche un terrorista ben addestrato avrebbe difficoltà a non mostrare \*alcun\* segno di nervosismo durante il controllo del suo documento di identità da parte di un funzionario di sicurezza in divisa. Purtroppo, immagino che molti impiegati della TSA non sono minimamente addestrati per identificare questo tipo di comportamento. Nell'esempio del bar, la bravura di quel tipo derivava da anni di osservazioni ed esperienza.

Naturalmente, questo "studio comportamentale" ha certi margini di errore, ma potrebbe essere molto utile per individuare un gruppo di persone che occorre controllare con più attenzione. È troppo sperare che la vera ragione del proliferare di tutti questi posti di controllo nella nostra società del dopo-11 settembre sia il fornire spunti per tale "studio comportamentale", e non una qualche illusione di massa attuata dai funzionari di sicurezza?

Da: DV Henkel-Wallace <[gumby@henkel-wallace.org](mailto:gumby@henkel-wallace.org)>  
Oggetto: Identificazione e sicurezza

I controlli sui documenti di identità sono ancora più dannosi e inutili di quanto lei stesso afferma. Nella maggior parte dei casi non serve nemmeno un documento falso -- è sufficiente uno autentico. Questi presunti "controlli" che vengono svolti negli ospedali, negli edifici governativi, nelle fiere (!), e così via, di solito non comportano alcuna verifica per vedere se il proprio nome è presente su una qualche lista particolare.

Controllano soltanto che abbiate con voi un documento che abbia qualche parvenza di identificazione valida. Per entrare in svariati edifici statali ho utilizzato finora la mia tessera scaduta del Price Club, la mia fototessera del Club Nazionale della Caccia (un documento scritto a mano, anche se \*è\* laminato), e così via. E perché no? Il "controllo" non verifica comunque niente su di me.

Che cosa si OTTIENE da tutto ciò? 1) Si tengono i senzاتetto al di fuori dei palazzi di giustizia, 2) Si impedisce a chi vuol restare anonimo di lasciare un messaggio al proprio senatore, e 3) Si va a consolidare una cultura che accetta la routine del "Documenti, prego".

Personalmente non credo che nessuno di questi risultati sia di qualche utilità, ma forse appartengo a una minoranza.

Da: "Bruce Ediger" <[eballen1@qwest.net](mailto:eballen1@qwest.net)>  
Oggetto: L'economia dello Spam

Salve. Ho letto con un certo interesse il numero di Crypto-Gram del 15 febbraio, in particolare modo il suo articolo intitolato "L'economia dello Spam".

Approvo che lei abbia parlato dello spam da un punto di vista economico, ma credo che le siano sfuggiti due aspetti.

1. Naturalmente Gates ha interesse che qualcuno paghi per inviare e-mail. È l'unico modo che ha Microsoft per far diventare la posta elettronica una miniera d'oro. Hanno già dei piani in corso per applicare una protezione anticopia (DRM) su tutte le macchine Windows, per cui probabilmente Gates ritiene che l'infrastruttura DRM potrebbe essere impiegata anche a livello di posta elettronica. Imporre una struttura di pagamento e di protezione anticopia sulle e-mail permette inoltre a Microsoft di abbattere SMTP, l'attuale standard libero di trasporto dell'e-mail. Gates è ben consapevole che i protocolli di uso quotidiano vengono copiati con estrema rapidità.

2. La redditività dello spam come pubblicità dipende da forze di mercato molto deboli per quella forma di propaganda. Lo spam ha questa proprietà davvero unica, e cioè che ogni destinatario contribuisce a pagare la pubblicità (in termini di tempo speso online, di cicli di

CPU, di spazio su disco, ecc.) ancor \*prima\* che la vittima dello spam abbia la possibilità di decidere se acquistare o meno il prodotto reclamizzato. Questo differisce completamente da ogni altra forma di pubblicità, eccezion fatta per il telemarketing e il junk faxing (ovvero avvisi pubblicitari via fax non richiesti). I cartelloni, gli spot televisivi e radiofonici, gli annunci su giornali e riviste, e il direct mailing obbligano l'inserzionista a sostenere il 100% dei costi. Naturalmente, quella piccola percentuale di persone che decide di acquistare il prodotto reclamizzato finirà con il pagare la pubblicità, ma rimane inalterato l'aspetto chiave: la scelta dell'acquirente. Una pubblicità convenzionale non deve offendere quasi tutti i potenziali acquirenti, altrimenti la Mano Invisibile punisce chi ha realizzato il prodotto che viene proposto. La Mano Invisibile del Mercato però influisce solo marginalmente sugli spammer, visto che una parte o la totalità dei costi dell'annuncio sono già stati sostenuti dai destinatari del messaggio.

Da: Ralf Holzer <[rholzer@cmu.edu](mailto:rholzer@cmu.edu)>  
Oggetto: Esenzioni dal programma US-VISIT e coefficienti di errore

Lei ha più volte sostenuto che tutte le nazioni estere, tranne 27, sono soggette alle misure di sicurezza (US-VISIT) che prevedono la presa di impronte digitali e di fotografie, ora vigenti in molti dei punti di accesso americani. Volevo solo far presente che queste esenzioni riguardano principalmente i turisti. Io sono uno studente diplomato proveniente dalla Germania e possiedo un visto F-1, e sono obbligato ad attenermi a quelle procedure di sicurezza. I turisti che provengono dalla Germania e da altre nazioni europee sono esentati solo perché tutti i passaporti europei dovranno avere delle identificazioni biometriche per poter entrare negli Stati Uniti a partire dall'autunno.

Un mio collega studente, che proviene da una nazione per cui è richiesta una speciale registrazione, mi ha raccontato che ormai egli ha svariati profili nel programma US-VISIT, perché il sistema continua a sbagliare l'identificazione delle sue impronte digitali. Il funzionario dell'Immigrazione sembrava non avere idea di come ovviare a questo problema. Questo elevato coefficiente di errore mi fa davvero dubitare dell'efficacia del programma US-VISIT.

Da: [rfleming@cultdeadcow.com](mailto:rfleming@cultdeadcow.com)  
Oggetto: I database delle tessere di fidelizzazione dei supermarket

Circa una settimana fa mi è arrivata della pubblicità proveniente dai supermercati Albertson, che annunciavano la creazione della loro nuova tessera di fidelizzazione. Il volantino dice: "La vertenza sindacale è stata dura per tutti. Ma una cosa sappiamo con certezza -- il giorno in cui finirà, inizierete a risparmiare come non mai. Gli sconti migliori e le offerte speciali saranno vostre... con la nuova tessera Albertsons Sav-on Preferred Savings Card. Abbonatevi subito!"

Questa cosa mi ha fatto pensare. Safeway e Ralph's (le altre due catene di supermercati colpiti dallo sciopero) hanno già delle tessere di fidelizzazione. Una cosa che LORO sanno con certezza è chi dei loro clienti si farà strada attraverso i picchetti per andare a far la spesa, e chi no.

In altre parole, gli schemi di acquisto contenuti nei database delle tessere di fidelizzazione di Safeway e Ralph's potrebbero essere FACILMENTE esaminati per controllare le simpatie dei singoli clienti verso il sindacato.

Riflettiamoci su. La prossima volta che qualcuno cercherà lavoro al supermercato Safeway o Ralph's della sua zona, dovrebbe aspettarsi che vengano controllate le sue abitudini nel fare la spesa nel periodo 2003-2004 per trovare indizi su una sua possibile posizione pro o contro il sindacato? E cosa impedisce a questi supermercati di offrire queste informazioni ad altre aziende o persino ai depositari del programma Total Information Awareness?

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

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

La versione italiana è curata da Communication Valley SpA

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

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

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

Per informazioni [crypto-gram@communicationvalley.it](mailto:crypto-gram@communicationvalley.it).

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

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

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

Copyright (c) 2004 by Bruce Schneier.