



password impossibili da indovinare. Per qualsiasi cosa che richieda una certa sicurezza, l'era delle password è finita.

L'autenticazione a due fattori risolve questo problema. Funziona contro gli attacchi passivi: l'intercettazione e i software che indovinano le password. Protegge da quelle problematiche generate da utenti che scelgono password deboli, o che le riferiscono ai loro colleghi di lavoro, o che le scrivono su pezzi di carta attaccati ai loro monitor. Per un'organizzazione che cerca di migliorare il controllo di accesso dei propri impiegati, l'autenticazione a due fattori è un'ottima idea. Microsoft sta integrando l'autenticazione a due fattori nel proprio sistema operativo, un'altra ottima idea.

Quel che l'autenticazione a due fattori non può fare è prevenire i furti di identità e le frodi. Può prevenire determinate tattiche di furto d'identità e di frode, ma i criminali cambieranno semplicemente il loro modus operandi. Si stanno già vedendo tattiche di frode che eludono completamente l'autenticazione a due fattori. A mano a mano che le banche adotteranno questo tipo di autenticazione, i criminali passeranno a nuove tattiche d'attacco.

Un modo di affrontare la questione è quello di pensare al fatto che l'autenticazione a due fattori risolve i problemi di sicurezza che riguardano appunto l'autenticazione. L'attuale ondata di attacchi a sistemi finanziari non sta sfruttando vulnerabilità nel sistema di autenticazione, per cui l'autenticazione a due fattori non è d'aiuto.

La sicurezza è sempre un braccio di ferro, e si potrebbe affermare che questa situazione si tratti semplicemente del costo del mantenersi a galla. Il problema di questa linea di pensiero è che non tiene conto delle contromisure atte a ridurre le frodi in maniera permanente. Concentrandosi sull'autenticazione dell'individuo invece che sull'autenticazione della transazione, le banche sono costrette a difendersi contro tattiche di attacco criminali e non contro il reato stesso.

Le carte di credito sono un esempio perfetto. Si noti quanta poca attenzione viene prestata all'autenticazione del possessore della carta. I commessi nei negozi controllano a malapena la firma. In molti usano le proprie carte tramite telefono e Internet, dove non viene nemmeno verificata l'esistenza della carta stessa. Le compagnie delle carte di credito investono in sicurezza autenticando la transazione, non il possessore della carta.

L'autenticazione a due fattori è una soluzione attesa da lungo tempo al problema delle password. Mi fa piacere la sua crescente diffusione, ma i furti di identità e le frodi bancarie non sono i risultati di problemi a livello di password ma sono altresì generati da transazioni autenticate in modo pessimo. Prima verrà compreso questo problema, prima si smetterà di sostenere misure di autenticazione più forti e quindi si otterrà un miglioramento in termini di sicurezza.

Questo articolo è originariamente apparso in Network World nell'ambito di un "faccia a faccia":  
<<http://www.nwfusion.com/columnists/2005/040405faceoff-counterpane.html>>  
oppure <<http://tinyurl.com/5nuod>>

Joe Uniejewski di RSA Security ha sostenuto una posizione opposta:  
<<http://www.nwfusion.com/columnists/2005/040405faceoff-rsa.html>>

Un'altra confutazione:  
<<http://www.eweek.com/article2/0,1759,1782435,00.asp>>

Ulteriori notizie:  
<[http://searchsecurity.techtarget.com/originalContent/0,289142,sid14\\_gci1077406,00.html](http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1077406,00.html)>  
oppure <<http://tinyurl.com/5tp6u>>



e gli effetti della sostituzione di persona a livello telematico, occorre concentrarsi sulla prevenzione e il rilevamento di transazioni fraudolente.

Queste non hanno niente a che fare con i legittimi intestatari dei conti. I criminali impersonano i legittimi intestatari quando si relazionano con le istituzioni finanziarie. Ciò vuol dire che qualsiasi soluzione non può coinvolgere gli intestatari dei conti. Di conseguenza può esserci soltanto una risposta sensata: che le istituzioni finanziarie siano ritenute responsabili per le transazioni fraudolente. Devono essere ritenute responsabili per aver inviato alle agenzie di credito informazioni errate basate su transazioni fraudolente.

Non possono sostenere che debba essere l'utente a tenere al sicuro la propria password, o il proprio sistema esente da virus. Non possono richiedere all'utente di controllare i propri conti alla caccia di attività fraudolente, o i propri estratti conto per verificare che non siano state richieste carte di credito in modi fraudolenti. Per moltissimi utenti, questi non sono requisiti ragionevoli. La banca deve essere ritenuta responsabile, a prescindere da quel che fa l'utente.

Se pensate che questo non possa funzionare, osservate le carte di credito. Le compagnie di carte di credito sono responsabili di tutto tranne i primi 50 dollari di transazioni fraudolente. A loro non manca certo un volume d'affari, e allo stesso tempo non sono certo sommerse dalle frodi. Hanno sviluppato e messo in campo una serie di tecnologie di sicurezza pensate per rilevare e prevenire transazioni fraudolente. Hanno spinto la maggior parte dei costi attuali sui commercianti. E quasi nessuna sicurezza è incentrata sul tentativo di autenticazione del possessore della carta di credito.

È una lezione importante. Le soluzioni ai furti di identità si focalizzano troppo sull'autenticazione dell'individuo. Che si tratti di autenticazione a due fattori, carte d'identità, biometria o che altro, esiste un mito assai diffuso secondo cui autenticare la persona sia il sistema per prevenire questo genere di reati. Ma una volta compreso che il problema sono le transazioni fraudolente, ci si rende subito conto di come l'autenticazione dell'utente non sia la via da seguire.

Pensiamo ancora alle carte di credito. I commessi dei negozi verificano a malapena le firme quando la gente le adopera. Le carte di credito possono essere utilizzate per acquistare via posta ordinaria, per telefono o via Internet, dove nessuno verifica la firma e nemmeno che voi siate davvero in possesso della carta. Inoltre nessuna compagnia di carte di credito impone dei requisiti per una conservazione sicura della carta di credito. Non è richiesto al titolare della carta di mettere in sicurezza il proprio portafoglio in qualche maniera particolare. Le compagnie di carte di credito semplicemente non si curano di verificare il titolare di una carta o di imporre regole su quel che fa. Si concentrano invece sulla verifica della transazione.

La stessa linea di pensiero deve essere impiegata in tutte le altre aree in cui i criminali si servono della sostituzione di persona per commettere una frode. Non so dire come saranno le soluzioni finali, ma so che dal momento in cui le istituzioni finanziarie saranno responsabili delle perdite causate da questo tipo di frodi, allora troveranno di sicuro delle soluzioni. Forse ci sarà un limite di prelievo giornaliero, come già esiste nei Bancomat. Forse transazioni più cospicue saranno ritardate per un certo intervallo di tempo, o richiederanno una chiamata da parte della banca o dell'intermediario. Forse la gente non sarà più in grado di attivare una carta di credito semplicemente riempiendo un modulo di informazioni. Probabilmente la soluzione finale sarà una combinazione di soluzioni che riducono le transazioni fraudolente a livelli gestibili, ma non lo sapremo mai finché le istituzioni finanziarie non avranno l'incentivo economico per metterle in atto.

Ora come ora, gli incentivi economici fanno sì che le istituzioni finanziarie sono talmente entusiaste di permettere transazioni di ogni tipo (nuove carte di credito, trasferimenti di denaro, ecc.) che non stanno prestando sufficiente attenzione alle transazioni fraudolente. Hanno spinto i costi delle frodi sui commercianti. Ma se vengono ritenute responsabili delle perdite e dei danni



<<http://www.cryptogram.it/aprile02.htm#a6>>

I vantaggi naturali della difesa: che cosa può insegnare la storia militare alla sicurezza delle reti, prima parte:

<<http://www.schneier.com/crypto-gram-0104.html#1>>

Lo Uniform Computer Information Transactions Act (UCITA):

<<http://www.schneier.com/crypto-gram-0004.html#ucita>>

Crittografia: l'importanza di non essere diversi:

<<http://www.schneier.com/crypto-gram-9904.html#different>>

Minacce ai danni delle smart card:

<<http://www.schneier.com/crypto-gram-9904.html#smartcards>>

Attaccare i certificati con virus informatici:

<<http://www.schneier.com/crypto-gram-9904.html#certificates>>

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

I nuovi rischi della biometria

È il tipo di attacco di cui abbiamo parlato sin dall'avvento della biometria. In Malaysia, dei criminali hanno tagliato il dito di un uomo per aprire la serratura biometrica della sua Mercedes.

Quel che mi interessa sottolineare di questa storia è l'interazione fra aggressore e difensore. Il difensore mette in atto una contromisura che costringe l'aggressore a cambiare tattica. A volte la nuova tattica risulta essere più pericolosa e dannosa, e non è affatto ovvio se la contromisura sia stata sufficientemente valida da giustificarlo.

In "Beyond Fear" ho scritto in merito a una simile problematica (pag. 113): "Qualcuno potrebbe pensare: 'Mi preoccupa il fatto che possano rubarmi l'auto, allora comprerò un costoso dispositivo di sicurezza che rende impossibile l'avviamento del motore usando i cavetti'. Sembra una linea di pensiero ragionevole, ma in paesi come la Russia, dove questi dispositivi sono molto comuni, si è visto un aumento dei furti d'auto commessi con la forza. Prendere l'auto a qualcuno con violenza espone il proprietario della macchina ad un rischio maggiore; in questo caso, la misura di sicurezza ha spostato l'anello debole della catena dal motorino di avviamento al proprietario del veicolo. Il numero totale di furti d'auto sarà anche diminuito, ma anche la sicurezza dei proprietari".

È certamente possibile progettare dei lettori di impronte digitali che verifichino la "vitalità": pulsazioni, temperatura corporea, ecc., ma queste nuove misure di sicurezza porteranno a nuove tattiche di aggressione, e il ciclo continuerà.

<<http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm>>

\*\* \*\* \*\* \*\*~

News

Malfunzionamenti dei sensori antiterrorismo:

<[http://www.nti.org/d\\_newswire/issues/print.asp?story\\_id=ABE17A0A-395C-4FA9-9B34-D02CA791679F](http://www.nti.org/d_newswire/issues/print.asp?story_id=ABE17A0A-395C-4FA9-9B34-D02CA791679F)> oppure <<http://tinyurl.com/3mxy5>>

Specifiche dei passaporti elettronici statunitensi:

<<http://a257.g.akamaitech.net/7/257/2422/01jan20051800/edocket.access.gpo.gov/2005/05-3080.htm>> oppure <<http://tinyurl.com/55gna>>

Hacker che prendono il controllo delle webcam:

<[http://www.theregister.co.uk/2005/02/28/webcam\\_trojan\\_case/](http://www.theregister.co.uk/2005/02/28/webcam_trojan_case/)>

Una storia di ingegneria sociale all'IRS:

<<http://www.cnn.com/2005/TECH/03/17/irs.computer.security.ap/index.html>>  
oppure <<http://tinyurl.com/5722f>>

Un articolo che tratta di certe sciocche e inutili segretezze imposte dal governo degli Stati Uniti per motivi di sicurezza (richiede autenticazione):

<<http://online.wsj.com/article/0,,SB111145546123985866,00.html>>

L'articolo spiega come ai piloti non sia permesso di volare nelle vicinanze di centrali nucleari, ma allo stesso tempo non è permesso dire ai piloti dove si trovino le centrali nucleari. Ecco la storia di come un individuo ha scoperto l'esatta ubicazione della centrale nucleare di Oyster Creek nel New Jersey usando solamente informazioni disponibili pubblicamente.

<<http://synflood.at/blog/archives/2005:03:28/how-to-find-nuclear-power-plants>>  
oppure <<http://tinyurl.com/63nkr>>

Un buon articolo di opinione sui problemi di sicurezza legati alla segretezza:

<[http://www.independent-media.tv/item.cfm?fmedia\\_id=10500&fcategory\\_desc=Top%20Stories%20Ignored%20By%20U.S.%20Media](http://www.independent-media.tv/item.cfm?fmedia_id=10500&fcategory_desc=Top%20Stories%20Ignored%20By%20U.S.%20Media)> oppure <<http://tinyurl.com/5jrby>>

Requisiti per i documenti d'identità di chi vota. I sostenitori dei documenti con fototessera da utilizzarsi ai seggi dimenticano che non tutti ne hanno uno. Non tutti prendono aerei. Non tutti hanno una patente di guida. Se un documento d'identità con fototessera è richiesto per votare, allora è meglio che sia 1) gratuito e 2) facilmente ottenibile ovunque e da tutti. Altrimenti diventa una tassa elettorale.

<<http://www.npr.org/templates/story/story.php?storyId=4558628>>

Uno studio dimostra (ancora una volta) come sia facile raccogliere informazioni personali da usare per commettere furti di identità.

<<http://news.bbc.co.uk/1/hi/technology/4378253.stm>>

Anonimato e Internet:

<<http://slate.com/id/2115120/>>

<[http://wendy.seltzer.org/blog/archives/2005/03/19/nyt\\_catches\\_the\\_anonymous\\_wifi\\_is\\_evil\\_bug.html](http://wendy.seltzer.org/blog/archives/2005/03/19/nyt_catches_the_anonymous_wifi_is_evil_bug.html)> oppure <<http://tinyurl.com/4kx34>>

Ottimo articolo che sostiene come il furto di identità sia inevitabile:

<[http://www.theregister.co.uk/2005/03/23/id\\_theft\\_cannot\\_be\\_escaped/](http://www.theregister.co.uk/2005/03/23/id_theft_cannot_be_escaped/)>

Perché le telecamere di sorveglianza non fanno diminuire i reati:

<<http://gritsforbreakfast.blogspot.com/2005/03/why-surveillance-cameras-dont-reduce.html>>  
oppure <<http://tinyurl.com/4r9qt>>

Sybase minaccia di perseguire legalmente i ricercatori che hanno scoperto vulnerabilità nei suoi prodotti:

<<http://www.computerworld.com/securitytopics/security/holes/story/0,10801,100637,00.html>>  
oppure <<http://tinyurl.com/67qdb>>

L'analisi di EPIC della nuova carta di identità multifunzione del Dipartimento per la Sicurezza Nazionale:

<<http://www.epic.org/privacy/surveillance/spotlight/0405.html>>

Un articolo di giurisprudenza sul costo dell'impedimento della divulgazione di informazioni sulle vulnerabilità:

<[http://www.digital-law.net/IJCLP/Cy\\_2004/ijclp\\_webdoc\\_10\\_Cy\\_2004.htm](http://www.digital-law.net/IJCLP/Cy_2004/ijclp_webdoc_10_Cy_2004.htm)>  
oppure <<http://tinyurl.com/4uy2q>>

Un aggressore attacca una banca dall'interno, servendosi di un registratore di input da tastiera:

<<http://news.bbc.co.uk/1/hi/uk/4356661.stm>>

Un altro attacco dall'interno, a opera di impiegati di un call center in India:

<[http://timesofindia.indiatimes.com/articleshow/msid-1070986\\_curpg-1.cms](http://timesofindia.indiatimes.com/articleshow/msid-1070986_curpg-1.cms)>  
oppure <<http://tinyurl.com/67hf2>>

Sandia ha pubblicato un rapporto, razionale e agghiacciante, sulla sicurezza antiterrorismo. L'ho commentato qui:

<[http://www.schneier.com/blog/archives/2005/04/sandia\\_on\\_terro.html](http://www.schneier.com/blog/archives/2005/04/sandia_on_terro.html)>

La London School of Economics ha recentemente pubblicato un rapporto sulle proposte del governo britannico in merito ai documenti d'identità nazionali. Una lettura decisamente consigliata.

<<http://www.lse.ac.uk/collections/pressAndInformationOffice/PDF/IDreport.pdf>>  
oppure <<http://tinyurl.com/4wxw3>>

In Texas: automobili con chip RFID incorporati:

<<http://gritsforbreakfast.blogspot.com/2005/04/tag-texas-cars-with-rfids-i-couldnt.html>> oppure  
<<http://tinyurl.com/5den8>>

Questi commenti sulla sicurezza dei passaporti elettronici sono un ... eccellente sui pericoli della tecnologia. Da leggere assolutamente l'Allegato 1: "Security and Privacy Issues in E-Passports" [Problematiche di Sicurezza e Privacy nei Passaporti Elettronici], uno studio un po' più tecnico a cura di Ari Juels, David Molnar, e David Wagner.

<[http://www.epic.org/privacy/rfid/rfid\\_passports-0405.pdf](http://www.epic.org/privacy/rfid/rfid_passports-0405.pdf)>

Ottimo articolo dell'Economist sulla sicurezza come compromesso:

<[http://economist.com/opinion/displayStory.cfm?story\\_id=3789466&CFID=50676895&CFTOKEN=39fd1de-3dfe5744-5457-4f96-aed8-20d51cefca2](http://economist.com/opinion/displayStory.cfm?story_id=3789466&CFID=50676895&CFTOKEN=39fd1de-3dfe5744-5457-4f96-aed8-20d51cefca2)>

Estratto: <[http://www.schneier.com/blog/archives/2005/04/security\\_as\\_a\\_t.html](http://www.schneier.com/blog/archives/2005/04/security_as_a_t.html)>

Abbiamo visto come sia possibile intercettare comunicazioni Bluetooth fino a un miglio di distanza. La novità è che ora si possono trovare le istruzioni passo-passo per costruirsi un apparecchio intercettatore per meno di 400 dollari. Che aspettate a costruirvene uno?

<<http://www.tomsnetworking.com/Sections-article106.php>>

C'è qualcuno che sia in grado di fornire un'argomentazione sensata che dimostri come il RFID non possa essere egualmente intercettabile?





su un foglio distinto.

Poi vi è la fase di "post-scrutinio". Gli Scrutatori fanno la somma di tutti i voti e determinano se vi è un vincitore. Poi i Revisori controllano l'intera procedura: schede, conteggi, tutto quanto. Infine le schede vengono bruciate (ecco da dove viene il fumo: fumata bianca se è stato eletto un Pontefice; nera in caso negativo).

Quanto è difficile da boicottare tutto questo processo? La prima osservazione da fare è che il sistema è completamente manuale, e quindi immune da quei tipi di attacchi tecnologici che rendono così rischiosi i sistemi di voto moderni. La seconda osservazione è che il ristretto gruppo di votanti -- i quali si conoscono tutti -- rende impossibile l'intervento di un sabotatore esterno. La Cappella viene sgombrata e chiusa a chiave prima del voto. Nessuno può travestirsi da cardinale e intrufolarsi nella Cappella Sistina. A tutti gli effetti, il processo di verifica del votante è perfetto come non mai.

Un'intercettazione, un ascolto passivo di tutto il processo sono certamente possibili, anche se le regole stabiliscono esplicitamente che nella Cappella debba essere verificata la presenza di dispositivi di registrazione e di trasmissione "ricorrendo alla perizia di due tecnici di fiducia". Ho letto che il Vaticano è preoccupato dai microfoni laser, dato che vi sono delle finestre in prossimità del tetto della Cappella.

Questo ci lascia con la possibilità di attacchi dall'interno. Può un cardinale influenzare l'elezione? Di certo gli Scrutatori potrebbero, potenzialmente, modificare dei voti, ma è arduo. Il conteggio viene effettuato in pubblico, e vi sono molte persone atte a controllare ogni fase. È possibile che il primo Scrutatore, se è abile nei giochi di prestigio, riesca a scambiare una scheda con un'altra prima di conteggiarla. Oppure che il terzo Scrutatore scambi le schede durante il conteggio.

Un cardinale non può mettere voti fraudolenti nell'urna. Il complesso rituale del piatto e del recipiente assicura che ogni cardinale voti solamente una volta (la sua scheda è visibile) e che tenga la mano fuori dal recipiente con le altre schede.

Aumentare la dimensione delle schede renderebbe questi attacchi ancor più difficili. Stesso effetto sarebbe prodotto da un miglior controllo delle schede da utilizzare, distribuendone soltanto una per ogni cardinale. Presumibilmente i cardinali cambiano idea più spesso durante il processo di voto, per cui ha senso distribuire più schede per ciascuno.

Le schede di votazioni precedenti vengono bruciate, il che rende assai difficile usarne una per inquinare l'urna. Ma c'è una grinta: "Se però si dovesse procedere immediatamente ad una seconda votazione, le schede della prima votazione saranno bruciate solo alla fine, insieme con quelle della seconda votazione". Immagino che questo venga fatto in modo che vi sia soltanto una fumata per le due elezioni, ma sarebbe più sicuro bruciare ogni serie di schede prima del turno successivo di votazione (tuttavia l'intero mazzo di schede viene perforato da un ago e le schede legate insieme, il che 1) le contrassegna come già usate e 2) ne impedisce praticamente il riutilizzo).

E infine, i cardinali vestono l'"abito corale" durante il voto; tale abito presenta maniche di pizzo molto luminose coperte da una corta mantellina rossa: è molto arduo fare "giochi di prestigio" in queste condizioni.

È possibile che uno Scrutatore alteri la registrazione dei voti, ma con tre Scrutatori la discrepanza verrebbe subito notata. Presumo che si passerebbe subito a un secondo conteggio, e verrebbe ripristinato il registro corretto. Due o tre Scrutatori in combutta fra loro potrebbero provocare più danni, ma dato che gli Scrutatori vengono estratti a caso, le probabilità che vengano scelti tre Scrutatori corrotti sono bassissime. E comunque i Revisori controllano tutto.

Più interessante sarebbe provare ad attaccare il sistema di selezione degli Scrutatori, che non viene definito con chiarezza nel documento. Influenzare la selezione di Scrutatori e Revisori sembra essere un primo passo necessario se si intende boicottare l'elezione.

Schede con più di un nome vengono annullate, e presumo avvenga lo stesso nel caso di schede senza nome (bianche). Schede illeggibili o ambigue sono forse le più frequenti, e suppongo che vengano scartate. Le regole hanno una disposizione precisa nel caso di più schede da parte dello stesso cardinale: "Qualora nello spoglio dei voti gli Scrutatori trovassero due schede piegate in modo da sembrare compilate da un solo elettore, se esse portano lo stesso nome vanno conteggiate per un solo voto, se invece portano due nomi diversi, nessuno dei due voti sarà valido; tuttavia, in nessuno dei due casi viene annullata la votazione". Questo mi sorprende, ma suppongo sia accaduto per errore.

Se vi è una fase debole, è quella del conteggio delle schede. Non c'è una vera e propria ragione di effettuare un preconteggio, e questo dà allo Scrutatore che si occupa del trasferimento la possibilità di scambiare schede legittime con altre che ha tenuto nascoste nella manica. Mi piace l'idea di mescolare le schede casualmente, ma metterle tutte in una gabbietta girevole farebbe ottenere lo stesso risultato in maniera più sicura, anche se meno cerimoniosa.

E se dovessi migliorare il processo, aggiungerei un qualche trattamento con guanti bianchi, per evitare che uno Scrutatore nasconda la punta di una matita o penna sotto le unghie. Anche se l'obbligo di scrivere per esteso il nome del candidato offre maggior resistenza a questo genere di attacco.

Il recente cambiamento che permette ai cardinali di andare e venire dalla Cappella alle proprie stanze (invece di rimanere rinchiusi nella Cappella durante l'intera elezione, come veniva fatto in precedenza) ha reso il processo un po' meno sicuro, ma di certo più confortevole.

Infine, uno degli Infirmarii può avere la possibilità di far quel che vuole quando trascrive il voto di un cardinale infermo, ma non c'è modo di prevenire questa evenienza. Se il cardinale è preoccupato che ciò possa accadere, potrebbe chiedere a tutti e tre gli Infirmarii di controllare il corretto procedimento.

Esistono poi enormi fattori scoraggianti di ordine sociale, anzi religioso, al boicottaggio del voto. L'elezione ha luogo all'altare di una cappella. I cardinali pronunciano una formula di giuramento mentre votano: altro disincentivo. Gli Scrutatori sono esplicitamente esortati a non formare alcun tipo di combriccola o di perpetrare piani per inquinare l'elezione, pena la scomunica: "i Cardinali elettori si astengano, inoltre, da ogni forma di patteggiamenti, accordi, promesse od altri impegni di qualsiasi genere, che li possano costringere a dare o a negare il voto ad uno o ad alcuni".

Sono sicuro che sussistano accordi, patti e influenze -- i cardinali sono comuni mortali, dopotutto, e cose del genere fanno parte del modo con cui gli esseri umani si accordano fra loro.

Quali sono gli insegnamenti, qui? Primo: sistemi aperti condotti all'interno di un gruppo conosciuto rendono più ardua un'eventuale frode. Ogni fase del procedimento dell'elezione viene osservata da tutti, e tutti si conoscono, il che rende praticamente impossibile che qualcuno la faccia franca. Secondo, elezioni semplici e di ristretta portata sono più facili da rendere sicure. Questo tipo di processo funziona per eleggere un Pontefice o il presidente di una società, ma diventa subito impraticabile per un'elezione su vasta scala. L'unico modo che permette ai sistemi manuali di funzionare è attraverso una struttura piramidale, dove gruppi ristretti riportano i rispettivi risultati ottenuti manualmente su fino alla cima della piramide, verso autorità di tabulazione più centralizzate.

Il terzo ed ultimo insegnamento: quando il procedimento per un'elezione è lasciato maturare nel corso di un paio di migliaia di anni, si finisce con l'ottenere qualcosa di sorprendentemente buono.

Le regole per l'Elezione Papale:

<[http://www.vatican.va/holy\\_father/john\\_paul\\_ii/apost\\_constitutions/documents/hf\\_jp-ii\\_apc\\_22021996\\_universi-dominici-gregis\\_en.html](http://www.vatican.va/holy_father/john_paul_ii/apost_constitutions/documents/hf_jp-ii_apc_22021996_universi-dominici-gregis_en.html)> oppure <<http://tinyurl.com/3ldzm>>

In italiano:

<[http://www.vatican.va/holy\\_father/john\\_paul\\_ii/apost\\_constitutions/documents/hf\\_jp-ii\\_apc\\_22021996\\_universi-dominici-gregis\\_it.html](http://www.vatican.va/holy_father/john_paul_ii/apost_constitutions/documents/hf_jp-ii_apc_22021996_universi-dominici-gregis_it.html)>

In questa pagina Web vi è una figura che mostra un abito corale:

<<http://dappledphotos.blogspot.com/2005/01/biretta-sightings.html>>

\*\* \*\*

Le News di Counterpane

Schneier è stato scelto da Infoworld come uno dei 25 maggiori CTO:

<[http://www.infoworld.com/article/05/04/11/15FEcto2005schneier\\_1.html?s=feature](http://www.infoworld.com/article/05/04/11/15FEcto2005schneier_1.html?s=feature)>  
oppure <<http://tinyurl.com/3pdsq>>

Counterpane ha annunciato una partner con MessageLabs per offrire servizi di e-mail sicura:

<<http://www.counterpane.com/pr-20050215b.html>>

\*\* \*\*

Il Canile: ExeShield

Ebbene sì, vi sono delle compagnie che credono che mantenere segreti gli algoritmi crittografici li renda più sicuri. "ExeShield si serve degli ultimi ritrovati in fatto di protezione software e tecnologia crittografica per garantire una protezione ancora maggiore delle vostre applicazioni. Naturalmente, per la vostra e nostra sicurezza, non comunicheremo a nessuno lo schema crittografico".

Il mio articolo che spiega perché la segretezza negli algoritmi crittografici non fa bene alla sicurezza:

<<http://www.schneier.com/crypto-gram-0205.html#1>>

\*\* \*\*

Secure Flight è nei guai

Rapporto N.1: Esiste un rapporto stilato dall'Ispettore Generale del Dipartimento per la Sicurezza Nazionale che sostiene che la TSA (Transportation Safety Administration) abbia mentito per quanto riguarda il proprio ruolo nell'ottenimento di informazioni personali di 12 milioni di passeggeri delle linee aeree allo scopo di testare Secure Flight.

Il rapporto non dice esplicitamente che la TSA ha mentito, ma così è stato.

Vale la pena leggere i dettagli. E quando li leggerete, ricordatevi che sono stati scritti proprio dallo stesso Ispettore Generale del Dipartimento per la Sicurezza Nazionale. Presumo che un investigatore più indipendente sarebbe stato ancor più severo. Non che il rapporto non sia severo, beninteso. Ecco alcuni passaggi principali da una storia della AP:

“Il rapporto cita diverse occasioni in cui i funzionari della TSA hanno rilasciato dichiarazioni non accurate in merito ai dati dei passeggeri:

Nel settembre 2003, lo staff del Freedom of Information Act dell'agenzia ricevette centinaia di richieste da parte dei passeggeri della linea JetBlue che intendevano sapere se la TSA aveva i loro dati. Dopo una ricerca sommaria, lo staff del FOIA (Freedom of Information Act) ha pubblicato una nota sul sito Web della TSA affermando che la TSA non aveva in suo possesso i dati dei passeggeri di JetBlue. Anche se lo staff del FOIA ha poi effettivamente trovato quei dati in maggio, la nota è rimasta sul sito per più di un anno.

Nel novembre 2003, il capo della TSA James Loy ha scorrettamente dichiarato al Comitato per gli Affari Governativi che certe tipologie di dati dei passeggeri non venivano utilizzate per testare il pre-screening dei passeggeri.

Nel settembre 2003 il reporter di una rivista di tecnologia ha chiesto a un portavoce della TSA se per testare il sistema di pre-screening dei passeggeri venissero usate delle informazioni reali. Il portavoce ha risposto che venivano utilizzati soltanto dati fasulli; le risposte “non erano molto precise”, era scritto nel rapporto”.

C'è di più. Il rapporto rivela che la TSA ha ordinato alla Delta Air Lines di consegnare i dati dei passeggeri nel febbraio 2002 per aiutare i Servizi Segreti a determinare se dei terroristi o loro affiliati stessero viaggiando in prossimità dei giochi Olimpici di Salt Lake City.

Viene rivelato, inoltre, che la TSA si è servita di dati dei passeggeri di JetBlue nella primavera del 2003 per capire come modificare il numero di persone da scegliere per un'ulteriore ispezione nell'ambito del sistema esistente.

Il rapporto sostiene che uno dei contraenti della TSA che lavoravano sul pre-screening dei passeggeri, Lockheed Martin, ha utilizzato un campione di dati proveniente da ChoicePoint.

Il rapporto inoltre illustra in dettaglio come i contraenti esterni abbiano usato i dati per propri scopi del tutto arbitrariamente e come “l'agenzia non si sia curata di richiedere la restituzione o la distruzione dei dati usati dai rivenditori”. Come “la TSA non abbia applicato in maniera efficace e coerente la protezione della privacy nel corso del proprio coinvolgimento nei trasferimenti dei dati dei passeggeri delle linee aeree”.

Questi sono fatti molto gravi. Dimostrano come la TSA abbia ripetutamente mentito all'opinione pubblica per quanto riguarda il suo uso di dati personali.

Rapporto N.2: Il GAO (Government Accountability Office) ha pubblicato un suo rapporto su Secure Flight. Lo scorso anno, il Congresso ha varato una legge che stabiliva che la TSA non avrebbe potuto implementare Secure Flight finché non rispettasse dieci condizioni: protezione della privacy, accuratezza dei dati, sovrintendenza, costo e garanzie per assicurare che il sistema non sia abusato o utilizzato da persone non autorizzate, e così via. Il rapporto del GAO ha stabilito che nove delle dieci condizioni non sono ancora state rispettate, e ha espresso forti dubbi sull'efficacia di Secure Flight.



tecnicamente avanzati; gli basta richiedere alla vittima una password usa-e-getta dal suo token di autenticazione tramite il solito trucco del finto sito Web, e usarla prima della scadenza. Nel caso particolare di schemi basati su "gettone" di convalida e non sul tempo, la finestra temporale disponibile potrebbe anche essere molto grande.

L'unica soluzione a questo problema è far passare le applicazioni bancarie dall'autenticazione utente all'esplicita autenticazione di ogni transazione. Per esempio, un token con una tastiera stile calcolatrice potrebbe invitare l'utente ad inserire direttamente il numero di conto del beneficiario e l'ammontare della somma da trasferire nel token stesso, e produrre quindi una password usa-e-getta che funge da MAC address di questi dettagli.

Il problema è che l'autenticazione della transazione è meno user-friendly e i token di autenticazione richiesti tendono ad essere più grandi e costosi. Ciononostante tali schemi sono sotto esame, soprattutto nell'ambito del Chip Authentication Program di MasterCard, che permette ai consumatori di utilizzare il loro Bancomat dotato di chip (più diffuso in Europa che negli Stati Uniti) unitamente ad un lettore di carta incorporato per fornire un'autenticazione a due fattori sia per l'utente che per la transazione.

L'SMS offre al consumatore non soltanto un canale separato, ma anche una interfaccia utente indipendente allo schermo del PC che è invulnerabile da attacchi Trojan e man-in-the-middle. Le password usa-e-getta via SMS possono quindi essere utilizzate non solo per l'autenticazione dell'utente, ma anche per autenticare la transazione, grazie a messaggi del tipo "Pagare 100 dollari al conto 12345? Codice di conferma: AGEWN".

Tutto questo è contenuto nel mio articolo "The Future of Phishing" (Il Futuro del Phishing) pubblicato quasi un anno fa e ancora disponibile, per esempio, a questo indirizzo:  
<<http://www.net-security.org/article.php?id=672>>

Da: Ernst Jan Plugge <[rmc@dds.nl](mailto:rmc@dds.nl)>  
Oggetto: I limiti dell'autenticazione a due fattori

Ho appena letto il suo interessante intervento sull'autenticazione a due fattori. Lei descrive un sistema in cui una banca invia un messaggio SMS per effettuare l'autenticazione e le relative debolezze. La mia banca fa qualcosa di simile, ma evita alcune di queste problematiche in maniera piuttosto elegante.

L'autenticazione verso l'applicazione Web della mia banca viene fatta semplicemente tramite password. All'interno dell'applicazione posso preparare tutta una serie di transazioni senza dover fornire ulteriori autenticazioni. Tuttavia, per confermare quella serie, devo fornire un TAN, ovvero un numero di transazione. Tale numero viene inviato via SMS al mio cellulare quando inizio la fase finale del processo e il messaggio comprende un riassunto della somma totale delle transazioni all'interno della serie, e un indice di numeri TAN ordinale, che aumenta di un'unità per ogni serie. Inserisco il numero e la serie viene processata. L'SMS, fra l'altro, è solo uno dei sistemi di invio supportati dalla banca. È anche possibile ottenere una lista di TAN stampata su carta e inviata per posta ordinaria. Le opzioni si escludono a vicenda.

Qualcuno che si impossessa sia della mia password che del mio cellulare può, ovviamente, mettermi nei guai. Ma un Trojan non avrà vita assai facile. Anzitutto, la semplice intercettazione e ripetizione non funzioneranno, perché il TAN è valido solo per una transazione. Un attacco di tipo man-in-the-middle dovrà controllare e dirottare le mie operazioni nell'applicazione Web in tempo reale e sostituire al volo i propri dati fraudolenti, dovrà inviare la sua serie di transazioni praticamente nello stesso momento in cui la sto inviando io e le cifre devono corrispondere esattamente. Perciò, anche se l'attacco man-in-the-middle avesse buon esito, i danni sono



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) 2005 by Bruce Schneier.