

CRYPTO-GRAM
15 maggio 2004

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

Edizione italiana curata da Communication Valley SpA

E-mail: schneier@counterpane.com
Web: <<http://www.schneier.com>> oppure <<http://www.counterpane.com>>

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

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

** **

In questo numero:

[I mandati come misure di sicurezza](#)
[Provvedimenti anti-terrorismo negli aeroporti](#)
[Le ristampe di Crypto- Gram](#)
[News](#)
[Le News di Counterpane](#)
[Note di sicurezza da ogni dove: evitare i Servizi Postali Statunitensi](#)
[Il Canile: Markland Technologies](#)
[Il Canile: IQ Networks](#)
[Consumatori della Sicurezza Nazionale](#)
[Commenti dei lettori](#)

** **

I mandati come misure di sicurezza

Anni fa, la parola "sorveglianza" significava detective con l'impermeabile che pedinavano le persone per strada.

I detective di oggi, molto più probabilmente, sono seduti davanti a un computer, e tutta la sorveglianza è ormai elettronica. È un sistema meno costoso, più semplice e più sicuro. Ma è anche più esposto ad eventuali abusi. Nell'universo della sorveglianza semplice e a buon mercato, un mandato offre ai cittadini un'importantissima sicurezza per difendersi da un'organizzazione di polizia più potente.

I mandati sono garantiti dal Quarto Emendamento e sono necessari prima che la polizia possa perquisire casa vostra o mettere sotto controllo il vostro telefono. Ma non è ancora ben chiaro quali altre forme di perquisizione e di sorveglianza siano contemplate dai mandati.

Un caso insolito e significativo avvenuto di recente in un tribunale di Nassau County ha messo in luce una parte dell'interrogativo: è richiesto un mandato prima che la polizia possa attaccare un dispositivo di tracciamento elettronico all'automobile di qualcuno?

È sempre stato possibile, per le forze dell'ordine, seguire un sospettato, e il tracciamento a distanza è vecchio di decenni. La sola differenza è che adesso è più facile e meno costoso utilizzare questa tecnologia.

La sorveglianza continuerà a diventare sempre più semplice e meno costosa, e soprattutto meno intrusiva. Nel caso di Nassau, la polizia ha nascosto un dispositivo di tracciamento su un'auto usata da un sospettato di furto, Richard D. Lacey. Dopo l'arresto di Lacey, il suo avvocato ha cercato di far eliminare le prove raccolte dal dispositivo di tracciamento sulla base del fatto che la polizia non aveva ottenuto un mandato che autorizzasse l'uso del dispositivo, e che quindi era stata violata la privacy di Lacey.

Il caso è stato ritenuto essere il primo di questo genere nello stato di New York e uno dei pochi a livello nazionale. Un giudice ha stabilito che la polizia avrebbe dovuto richiedere un mandato, ma si è rifiutato di escludere le prove sostenendo che il proprietario dell'auto era la moglie di Lacey, non lui, e che quindi Lacey non poteva reclamare alcuna privacy.

Sempre più, ci troviamo a vivere in una società dove tutti siamo controllati automaticamente in ogni momento.

Se la macchina usata da Lacey fosse stata equipaggiata con il sistema OnStar, avrebbe potuto essere controllata attraverso di esso. Ognuno di noi può essere tracciato tramite il proprio telefono cellulare. E-ZPass tiene traccia dei veicoli in corrispondenza di gallerie e ponti. Telecamere di sicurezza ci registrano quotidianamente. I nostri acquisti sono registrati dalle banche e dalle compagnie delle carte di credito, le telefonate che facciamo sono tracciate dalle compagnie telefoniche, le nostre abitudini nel navigare in Internet da chi opera nei vari siti Web.

Il Dipartimento di Giustizia sostiene di aver bisogno di questi (e altri) poteri di ricerca per contrastare il terrorismo. Un provvedimento inserito in un Appropriation Bill (legge di stanziamento) permette all'FBI di ottenere informazioni finanziarie private da banche, compagnie di assicurazioni, agenzie di viaggi, agenzie immobiliari, agenti di borsa, dal Servizio Postale Statunitense, da gioiellerie, casinò, concessionarie d'auto, il tutto senza un mandato.

A partire da quest'anno, il governo degli Stati Uniti ha deciso di prendere fotografie e impronte digitali di tutti i visitatori stranieri (ad eccezione di 27 nazioni) in ingresso alle frontiere americane. Il programma CAPPS II (Computer Assisted Passenger Prescreening System) proverà i precedenti di tutti i passeggeri che si imbarcano sui voli di linea. Durante il week-end di Capodanno l'FBI ha raccolto i nomi di 260.000 persone che risiedevano negli alberghi di Las Vegas. Sempre più spesso, la sorveglianza in stile "Grande Fratello" di Orwell sta diventando una realtà.

Purtroppo, spesso il dibattito viene erroneamente ridotto a una questione di quanta privacy occorre abbandonare per poter essere al sicuro. La gente si chiede: "Sarebbe meglio usare questa nuova tecnologia di sorveglianza per catturare terroristi e criminali, oppure dovremmo agire in favore della privacy e bandirne l'utilizzo?"

Questa è una domanda mal posta. Sappiamo che una nuova tecnologia offre alle forze dell'ordine nuove tecniche di ricerca, e rende le tecniche esistenti più economiche e semplici da usare. Sappiamo di essere tutti più sicuri quando la polizia può farne uso. E il Quarto Emendamento già permette le forme più invadenti di ricerca: la polizia può perquisire voi e casa vostra.

Quel che occorre sono altrettanti meccanismi per prevenire gli abusi. La formulazione corretta della domanda è questa: "Dovremmo permettere alle forze dell'ordine di utilizzare una nuova tecnologia senza alcuna supervisione imparziale, o dovremmo richiedere che siano controllate e che rendano conto delle proprie azioni?". E il Quarto Emendamento già ci predispone a questo nel suo obbligo di un mandato.

Il mandato di perquisizione (un obbligo di legge tecnologicamente neutrale) sostiene essenzialmente che, prima che la polizia possa aprire la posta, ascoltare telefonate o analizzare il flusso di dati alla ricerca di parole chiave, un "magistrato neutrale e imparziale" esamina le basi per la ricerca e si assume la responsabilità delle conseguenze. Le parole fondamentali qui sono: supervisione

News

Articolo interessante sull'uso dei vulnerability assessment per identificare problemi relativi a politiche di sicurezza:

< <http://www.onlamp.com/pub/a/security/2004/04/08/networksecurity.html> >

Il lungo messaggio e-mail di Bill Gates che descrive gli sforzi compiuti dalla sua azienda in merito alla sicurezza:

< <http://www.computerworld.com/printthis/2004/0,4814,91801,00.html> >

< <http://www.microsoft.com/mscorp/execmail/2004/03-31security-print.asp> >

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

Un'intervista ad Amit Yoran, direttore della Divisione Nazionale per la Cyber-Sicurezza del Dipartimento della Sicurezza Nazionale:

< <http://www.informationweek.com/shared/printableArticle.jhtml?articleID=18600292> >

oppure

< <http://tinyurl.com/2cetk> >

La TSA sta seriamente esplorando un programma "trusted traveler". Onestamente, non ne vedo molto la necessità. Le lunghissime code per la sicurezza che affliggevano gli aeroporti nei mesi successivi all'11 settembre sono in gran parte sparite, e i viaggiatori frequenti di classe superiore che aderiranno al programma hanno già una corsia preferenziale attraverso i controlli di sicurezza.

< <http://www.computerworld.com/securitytopics/security/story/0,10801,92099,00.html?nas=SEC-92099> > oppure < <http://tinyurl.com/3ybyt> >

Un buon articolo sulle compagnie di sicurezza che instillano paure per aumentare le vendite:

< <http://www.eweek.com/article2/0,1759,1566249,00.asp> >

Un lungo, ma ottimo studio sulle carte d'identità nazionali:

< http://books.nap.edu/html/id_questions/ >

Okay, è una cosa un po' grezza, ma è anche un'interessante idea della serie "sicurezza attraverso l'oscurità":

< <http://www.shomertec.com/item.cfm?Action=newItems&variable=1164> >

Sembra che la TSA possa abbandonare una delle regole aeroportuali dell'era post-11 settembre: solo i passeggeri muniti di biglietto sono ammessi ai controlli di sicurezza. Tale regola aveva un senso quando le code ai controlli di sicurezza erano lunghe; lasciando passare solo i passeggeri con biglietto significava avere meno persone in coda. Ma ora che le code si sono accorciate, questa regola non ha più senso. D'altro canto, la TSA sta effettuando i propri controlli "extra" ai checkpoint di sicurezza. Tutti coloro che non hanno biglietto saranno allora sottoposti a questi controlli "extra"?

< http://www.usatoday.com/travel/news/2004-04-19-airport-security_x.htm >

oppure < <http://tinyurl.com/yqax8> >

Nuovo brevetto NSA su un sistema key-escrow. Si noti che era stato richiesto nel 1996, quando questo genere di cose andava per la maggiore.

< <http://cryptome.org/nsa-access.htm> >

Un'interessante intervento sulle garanzie di "cyber-conformità". L'autore prende il concetto di "capacità di tenere il mare" applicato alle navi e cerca di applicarlo al software. È un modo di gestire le responsabilità. Vale davvero la pena leggerlo.

< <http://csdl.computer.org/comp/mags/sp/2004/02/j2073abs.htm> >

Come trasformare una macchina fotografica usa-e-getta in una pistola paralizzante.

< <http://www.techtv.com/unscrewed/ihateyou/story/0,24682,3653392,00.html> >

oppure

< <http://tinyurl.com/2xctm> >

Non ditelo a nessuno che lavori nella sicurezza aerea... Potrebbero iniziare a vietare le macchine fotografiche sugli aerei.

Più del 70% delle persone darebbe la propria password ad un estraneo in cambio di una tavoletta di cioccolato.

< <http://news.bbc.co.uk/2/hi/technology/3639679.stm> >

Questo genere di cose non mi sorprende. Pur aspettandomi che almeno alcune di quelle persone abbiano fornito una password falsa, sono sicuro che molti di loro hanno dato via le loro vere password.

Buona confutazione dell'articolo di Mossberg apparso sul Wall Street Journal riguardante le reti e la sicurezza informatica:

< <http://www.securityfocus.com/columnists/236> >

Un'interessante domanda e risposta con Paul Kocher. Peccato sia così corto.

< <http://zdnet.com.com/2100-1105-2-5201619.html> >

Un enorme sforzo di calcolo distribuito decodifica un problema crittografico a curva ellittica a 109 bit:

< http://www.theregister.co.uk/2004/04/29/crypto_certicom/ >

Buon articolo sullo spyware (si leggano anche le colonne laterali):

< <http://www.computerworld.com/securitytopics/security/story/0,10801,92784,00.html?SKC=home92784> > oppure < <http://tinyurl.com/2482t> >

Pare che la ricompensa offerta da Microsoft abbia contribuito alla cattura dell'autore del worm Sasser.

< <http://news.com.com/2100-7349-3-5208762.html> >

Un pezzo affascinante di crittanalisi side-channel: rompere chiavi RSA mediante l'ascolto dei computer.

< <http://www.wisdom.weizmann.ac.il/~tromer/acoustic/> >

Un'isola dove tutti sono costantemente sotto sorveglianza:

< <http://www.wired.com/news/privacy/0,1848,63316,00.html> >

La versione più recente di WinZip utilizza crittografia AES (AES-CTR e HMAC-SHA1, se volete i dettagli).

< http://www.winzip.com/aes_info.htm >

Purtroppo, la crittografia di WinZip è vulnerabile a svariati attacchi:

< <http://www.cse.ucsd.edu/users/tkohno/papers/WinZip/> >.

Morale (e non è certo una novità): la crittografia è una materia difficile, e non basta usare AES in un prodotto per renderlo magicamente sicuro.

** **

Le News di Counterpane

Bruce Schneier terrà un discorso alla Princeton University il 17 maggio:

< <http://webserv03.princeton.edu/cgi-bin/team/webevent.cgi?cmd=showevent&ncmd=listmonth&cal=cal282&id=30564> > oppure
< <http://tinyurl.com/2hxbf> >

Schneier interverrà alla EPIC's Freedom 2.0 Conference il 20 maggio:

< <http://www.epic04.org/> >

Schneier interverrà alla South Sound Technology Conference il 26 maggio:

< <http://www.sstconference.com/> >

Schneier interverrà ad una conferenza sulla sicurezza a Oslo il 2 giugno:
< <http://mnemonic.no/index.boom?cat=14&art=560> >

Intervista audio con Schneier:
< <http://www.itconversations.com/shows/detail119.html> >

I resoconti del primo trimestre di Counterpane:
< <http://www.counterpane.com/pr-20040827.html> >

Counterpane annuncia una partnership con Getronics:
< <http://www.counterpane.com/pr-20040512.html> >

Il webcast di Counterpane con Gartner:
< http://www.itworld.com/itwebcast/counterpane_msm/ >

** **

Note di sicurezza da ogni dove: evitare i Servizi Postali Statunitensi

Se siete il governo degli Stati Uniti, avrete certamente paura di ricevere posta all'antrace. Per cui sottoponete tutta la posta in ingresso a svariate procedure di controllo di sicurezza e di decontaminazione. Ma questo fa rallentare il flusso della posta. Allora siete costretti a dire alla gente come aggirare quelle procedure:

“La Commissione richiede che ogni commento o domanda redatti in forma cartacea vengano inviati tramite corriere o servizio “overnight”, se possibile, poiché la posta ordinaria nell'area di Washington e alla Commissione è soggetta a ritardi dovuti alle ristrette misure di sicurezza.”

Ora qualcuno potrebbe innescare una polemica dicendo che servizi come FedEx sono meno anonimi della posta ordinaria, ma non è vero. Chiunque con un numero di conto rubato o con una carta di credito può imbucare una lettera FedEx.

< <http://www.ftc.gov/os/2004/04/rfidworkshopfrn.pdf> >

** **

Il Canile: Markland Technologies

Ecco un'affascinante sito Web che parla del “sistema di trasmissione VYN a doppia cifratura senza chiave” (VYN Double Cipher Keyless Transmission System) di Markland Technologies. Gli scritti sono più letterariamente elevati del solito, ma presentano la maggior parte dei segnali di avvertimento della bufala standard: una profonda ignoranza in materia di crittografia da parte dell'autore, il solito algoritmo “perfetto”, il solito richiamo a calcoli matematici impressionanti, è stato esaminato e dichiarato corretto dal solito esperto senza nome, e la descrizione è assolutamente priva di dettagli illuminanti.

È interessante notare come l'autore ammetta che l'algoritmo presenti un inconveniente pratico: richiede 50 byte di overhead per trasmettere un byte di dati. Non c'è dubbio che l'essere “senza chiavi” rimedi a questa limitazione.

Inoltre, chiamare un prodotto "Crypto.com" quando non si possiede il dominio crypto.com pare quasi la formula per generare confusione.

< <http://www.marklandtech.com/crypto.html> >

** **

Il Canile: IQ Networks

In generale, il Canile è uno spazio dedicato a stupide aziende di sicurezza e/o ad altrettanto ridicoli prodotti di sicurezza. Crittografia da ciarlatani, sicurezza informatica senza senso, quel genere di cose. Ma questo mese abbiamo qualcosa di completamente diverso: una compagnia che commette una frode bella e buona.

IQ Networks dichiara di avere un impressionante comitato consultivo: Ross Anderson, Mihir Bellare, Steve Bellovin, Shafi Goldwasser, Peter Gutmann, Doug Stinson, Ron Rivest e Markus Kuhn. Disgraziatamente, nessuna di queste persone ha mai sentito nominare tale azienda. Né hanno dato il loro consenso per la pubblicazione di loro materiale sul sito. L'azienda dichiara inoltre di essere coinvolta nello Honeynet Project (nessuno dei ragazzi di Honeynet ne ha mai sentito parlare) e in Password Safe: e nemmeno io ho mai sentito parlare di questa gente.

IQ Networks ha anche un elenco impressionante di clienti. Scommetto quel che volete che sono tutti fasulli. Oh... sono sotto inchiesta da parte del SANS per aver piratato il materiale di addestramento del SANS.

Anche il resto del sito è assai divertente, con una gran quantità di generiche farneticazioni sulla sicurezza e scarsissime informazioni. La compagnia sostiene di fare pressoché di tutto e di più.

Compresterete i vostri servizi di sicurezza da un'azienda che mente praticamente su ogni cosa?

Il sito Web:

< <http://www.iq-net-works.com/> >

La lista dei clienti (difficile da trovare e che forse sarà presto cancellata):

< http://www.iq-net-works.com/clientes_english.html >

Peter Gutmann mi ha inviato questo link alcune settimane fa e ha denunciato la compagnia per l'uso illecito del suo nome. In risposta, la compagnia ha eliminato dal sito Web l'elenco di consulenti tecnici. Si è dimenticata, tuttavia, di eliminarlo dalla versione spagnola del sito.

< <http://www.iq-net-works.com/spanish/equipo.html> >

Fate in fretta, mi aspetto che anche questa pagina sarà presto eliminata.

È possibile dare uno sguardo al sito tramite archive.org, che ha salvato l'elenco di consulenti (anche in spagnolo) sin dal 2003. (Questo sito Web è ottimo per trovare vecchie versioni di pagine Web, oppure pagine Web che non esistono più).

< <http://web.archive.org/web/20030705082011/www.iq-net-works.com/equipo.html> > oppure

< <http://tinyurl.com/2dbwj> >

** **

Consumatori della Sicurezza Nazionale

La sicurezza nazionale è un argomento politico molto "caldo" ora, dato che entrambi i candidati alla presidenza ci chiedono di stabilire chi dei due sia la figura migliore per rendere sicuro il paese.

Molti dei vasti e costosi programmi governativi (CAPPS II, il sistema di tracciamento profili dei passeggeri delle linee aeree, il programma US-VISIT che prende le impronte digitali degli stranieri che entrano negli USA, nonché i vari programmi di data-mining in fase di ricerca e sviluppo) danno per scontato il bisogno di una maggiore sicurezza.

Alla fine del 2005, quando scadranno molti provvedimenti del controverso Patriot Act, ci verrà nuovamente richiesto di sacrificare certe nostre libertà in nome della sicurezza, visto che molti legislatori stanno puntando a rendere permanenti quei provvedimenti.

In qualità di esperto di sicurezza, noto che manca un componente essenziale al dibattito. È importante discutere di svariate misure di sicurezza, e determinare quali di esse saranno le più efficaci. Ma questo è solo metà dell'equazione; è altrettanto importante discutere dei costi. La sicurezza è sempre un bilanciamento, ed è a questo punto che sorge la vera domanda: "Questa misura di sicurezza vale quel che costa?"

In quanto americani e cittadini del mondo, dobbiamo pensare a noi stessi come utenti, come consumatori di sicurezza. Così come l'attento consumatore ricerca quel che è più conveniente per il proprio portafoglio, noi dobbiamo fare lo stesso. Molte delle contromisure proposte e implementate costano miliardi di dollari. Altre costano in altri modi: in termini di convenienza, privacy, diritti civili, libertà fondamentali, maggiori rischi di altre minacce. In quanto consumatori, abbiamo bisogno di ottenere più sicurezza possibile per quel che paghiamo.

L'invasione dell'Iraq, ad esempio, viene presentata come una mossa importante per la sicurezza nazionale. Può anche essere vero, ma è solo una parte della questione. Invadere l'Iraq è costato enormemente agli Stati Uniti. Il conto in denaro ammonta a più di 100 miliardi di dollari, ed è in continuo aumento. Il costo in vite umane ammonta a più di 600 americani, e le vittime continuano ad aumentare. Il costo in fatto di opinione mondiale è considerevole. E c'è una domanda a cui occorre dare risposta: "Era questo il modo migliore di spendere tutti quei soldi? In quanto consumatori di sicurezza, abbiamo forse ottenuto la maggior sicurezza possibile che potevamo ottenere da quei 100 miliardi di dollari, da tutte quelle vite, e da tutte quelle altre cose?"

Se quello è stato il modo migliore, allora abbiamo fatto la cosa giusta. Ma se non lo è stato, allora abbiamo commesso un errore. Anche se un Iraq libero è un fatto positivo a livello teorico, avremmo potuto essere più accorti e spendere meglio i nostri soldi, le nostre vite e la nostra buona volontà in qualche altra parte del mondo.

Questa è l'analisi corretta, ed è il modo in cui tutti pensano quando si tratta di compiere scelte legate alla sicurezza personale. Anche coloro che dicono che bisogna fare tutto il possibile per evitare un altro 11 settembre non sono d'accordo nel trattenere permanentemente a terra qualsiasi velivolo in questo paese. Anche se si trattasse di un'efficace misura di sicurezza, è una cosa ridicola. Non ne vale la pena. Abbandonare l'aviazione commerciale è un prezzo troppo alto da pagare per l'aumento di sicurezza che si acquisterebbe in cambio. Solo uno sciocco consumatore farebbe una cosa del genere.

Curiosamente, quando scrissi originariamente questo pezzo per CNet, ricevetti un commento che mi accusava di essere un pacifista. A mio avviso, si tratta di una considerazione fuori luogo. Non sto sposando una filosofia politica, ma una metodologia decisionale. Che siate pacifisti o militaristi, Repubblicani o Democratici, Americani o Europei, siete sempre consumatori di sicurezza. Ogni consumatore accetterà diversi compromessi e bilanciamenti, dato che molta di questa decisione è soggettiva, ma tutti si serviranno della medesima analisi.

E dobbiamo tener presente questa analisi quando pensiamo ad altre misure di sicurezza. La sicurezza aggiunta mediante l'impiego di CAPPS-II, il sistema di tracciamento profili dei passeggeri delle linee aeree, vale i miliardi di dollari che costerà, sia in denaro che nel sistematico stigmatizzare certe classi di americani? Non sarebbe più accorto spendere i nostri soldi per assumere traduttori arabi all'interno di FBI e CIA, oppure per aumentare le capacità di risposta alle emergenze nelle nostre metropoli e cittadine?

In quanto consumatori di sicurezza, dobbiamo compiere questa scelta. L'America non ha denari e libertà infiniti. Se dobbiamo spenderli entrambi per ottenere sicurezza, dobbiamo agire da consumatori intelligenti e puntare alla maggior sicurezza possibile.

L'efficacia di una misura di sicurezza è importante, ma non è l'unico fattore da tener presente. Quasi nessuna delle persone che stanno leggendo questo scritto indossa giubbetti antiproiettile. E non perché non funzionano (funzionano benissimo, se è per questo) ma perché la maggior parte delle persone non crede che valga la pena farlo. Non ne vale il costo, non ne vale la scomodità o la mancanza di stile. Il rischio che qualcuno ci spari è basso. In quanto consumatori di sicurezza, non riteniamo che un giubbotto antiproiettile sia un buon compromesso di sicurezza.

Allo stesso modo, molto di quanto viene proposto come sicurezza nazionale è un pessimo compromesso di sicurezza. Non ne vale la pena, e in quanto consumatori di sicurezza ci stanno fregando.

Non è facile essere un attento consumatore di sicurezza, così come non è facile essere un cittadino modello. Perché? Perché in entrambi i casi è richiesta una profonda considerazione di compromessi e alternative. Ma in questo anno di elezioni, tutto ciò è assolutamente importante. Dobbiamo informarci sulle problematiche. Dobbiamo rivolgerci ad esperti imparziali, che non stanno cercando di essere eletti o di rimanere eletti. Dobbiamo diventare persone informate. Altrimenti è come entrare in una concessionaria d'auto senza sapere nulla dei diversi modelli e dei prezzi, verremo sicuramente fregati.

Questo articolo è apparso originariamente, in forma ridotta, su News.com:
< <http://news.com.com/2010-7348-5204924.html> >

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

Commenti dei lettori

Da: Alan Morgan <amorgan@CS.Stanford.EDU>
Oggetto: Vincere illegalmente alle elezioni

Vincere illegalmente alle elezioni porta con sé un grosso rischio. Fare in modo che il vostro partito politico semiconosciuto ottenga il 5% del voto popolare, e quindi si qualifichi per ricevere i fondi integrativi federali, è meno rischioso. Ammettiamo che il Partito dei Verdi o dei Liberali ottenga il 5% del voto popolare alle prossime elezioni. Sarà un segno che questi partiti stanno acquisendo consensi fra il pubblico americano, o un segno che un ingegnere software fuori di testa ha deciso di far loro un regalo per l'anno elettorale?

Da: Robert <raven@ioa.com>
Oggetto: Vincere illegalmente alle elezioni

Nelle varie discussioni sulla sicurezza delle macchine per il voto elettronico che mi è capitato di leggere, molta attenzione sembra riservata alla vulnerabilità delle macchine nei confronti di azioni di "hacking" per alterare il numero dei voti.

Ecco uno scenario alternativo: per cambiare i risultati di un'elezione, distruggere i voti del partito opposto non è altrettanto efficace dell'aggiungere voti al proprio partito? Basta prendere di mira quelle macchine situate in zone in cui il vostro avversario presenta un grande vantaggio (l'area è nota per essere radicalmente a favore dell'uno o dell'altro partito) e fare in modo che vadano fuori uso e perdano i dati.

Questa mi sembra una cosa più semplice da fare che modificare il codice stesso. E dato che le macchine non tengono un registro cartaceo né un backup, non c'è modo di scoprire a chi appartenevano i voti.

Si aspetterebbe naturalmente l'ultimo momento nel giorno delle elezioni per avere il massimo effetto possibile. Tuttavia occorrerebbero dei gruppi di persone per mettere in atto tutto questo, dato che una o poche persone non sarebbero in grado di accedere a più di una macchina, o di entrare in più di un seggio elettorale, anche se si potrebbero usare falsi documenti di identità per facilitarsi le cose.

Le macchine potrebbero venire danneggiate con un piccolo "Zapper" a batteria, un po' come una pistola paralizzante portatile. Se colpiti nel posto giusto, i dati saranno cancellati, o comunque i circuiti saranno sufficientemente bruciati da rendere i dati illeggibili.

Questo sistema potrebbe suscitare un certo allarme dopo le elezioni, specialmente se si dimostra come le macchine operanti in certe aree abbiano avuto un tasso di malfunzionamento maggiore rispetto ad altre aree. Ma, come hanno mostrato i sistemi giudiziari, che cosa si potrebbe fare esattamente per porvi rimedio? Non staranno certo a rifare le elezioni da capo.

Questo sistema probabilmente non sarà molto pratico a livello nazionale o statale, ma potrebbe avere un certo impatto in caso di elezioni cittadine o locali.

Da: Ethan Sommer <sommere@ethanet.com>
Oggetto: Vincere illegalmente alle elezioni

Nella sua analisi, lei mette a confronto mele e arance. Il denaro speso per una campagna può essere sia del candidato stesso, oppure frutto di limitate donazioni (2000 dollari per candidati presidenziali) e ne viene accuratamente tenuta traccia. Se qualcuno volesse spendere quel denaro illegalmente, potrebbe (e anzi farebbe meglio a) utilizzare il denaro di persone che hanno voluto donare più di 2000 dollari (e forse molti di più), senza toccare i soldi presenti sul conto di cui si tiene accuratamente traccia.

A riprova di questo, lei sa quanti soldi hanno accumulato: dai 3 agli 8 milioni di dollari. Non crede che qualcuno si accorgerebbe se mancasse un milione di dollari? Potenzialmente c'è molto più denaro spendibile per una campagna illegale che non per una legale, perché non vengono applicate le leggi di riforma dei finanziamenti elettorali.

C'è poi la possibilità che una facoltosa "parte interessata" (un'azienda o un singolo individuo) possa spendere il proprio denaro per "sistemare" un'elezione senza che il candidato ne sia al corrente.

Da: Ethan Benatan <ethan.benatan@reed.edu>
Oggetto: Vincere illegalmente alle elezioni

Sembra che il valore del risultato di un'elezione possa essere legato solo marginalmente all'investimento (storicamente e pubblicamente) fatto nel tentativo di vincerla. I finanziamenti elettorali, anche negli USA, sono controllati in maniera piuttosto stretta dalla legge. Un valore effettivo potrebbe essere meglio valutato dall'influenza ottenuta dalla persona che entra in carica. Questo sarebbe certamente un elemento di previsione migliore del valore di un voto scambiato.

Bisogna anche notare come i potenziali aggressori formino un gruppo ben più ampio dei candidati stessi. In molti casi sono anche meno avversi al rischio e dispongono di maggiore liquidità.

Da: Pierre Szwarc <pierre.szwarc@laposte.net>
Oggetto: Documenti d'identità nazionali

Essendo un cittadino francese e vivendo in Francia, avere sempre con me un documento identificativo è obbligatorio. Lei ha ragione, non apporta alcun vantaggio per la sicurezza ordinaria. Però non va nemmeno ad aumentare i ritardi e gli ostacoli, come lei sembra temere. In tutti i miei 59 anni, mi è stata richiesta la carta d'identità dalle autorità esattamente *una volta*, e in circostanze in cui non mi sentivo obbligato a dimostrare di essere me. E questo accadde nel 1961, quando gli attacchi terroristici dei Nazionalisti Algerini (l'OAS) erano all'ordine del giorno. In svariate circostanze mi è stato chiesto di provare la mia identità, e in queste occasioni la carta d'identità si rivela molto comoda, e si adopera nell'identico modo in cui un cittadino statunitense userebbe la propria patente di guida: per bere alcolici in un bar appena ero in età per farlo, ad esempio, oppure per aprire un conto in banca. Vista da una prospettiva europea, la preoccupazione dell'americano medio per quanto riguarda la propria privacy in luoghi pubblici (come esemplificano film e telefilm), sembra più che altro una reazione esagerata verso una minaccia inesistente. Avendo subito la dominazione nazista per quasi sei anni, e anche se la generazione che ha sofferto direttamente quei terribili anni è in via di estinzione, il cittadino francese medio probabilmente non tollererebbe il Patriot Act così come è stato imposto a voi, e quindi la vostra preoccupazione per un'inezia come la carta d'identità sembra una cosa ridicola ai nostri occhi.

Da: Pierre Honeyman <phoneyman@telus.net>
Oggetto: Documenti d'identità nazionali

“Shake Hands with the Devil” [Stringere la mano al Diavolo], il resoconto del generale Romeo D'Allaire sul genocidio in Ruanda, racchiude un motivo ancor più agghiacciante per rifiutare documenti d'identità nazionali.

Gli autori del genocidio in Ruanda hanno utilizzato le carte d'identità sia per trovare le vittime del loro genocidio, sia per poi cancellare ogni traccia della loro esistenza. Le carte sono state controllate per assicurarsi che si stavano per uccidere le persone giuste, e poi sono state bruciate; nel frattempo, alcuni burocrati complici hanno rimosso ogni registrazione delle vittime dai database nazionali, facendo in modo che i registri confermassero che quelle persone non erano mai esistite.

Il solo pensiero che questo possa essere un potenziale utilizzo dei documenti d'identità nazionali è raggelante.

Se da un lato asserire che una cosa del genere non accadrebbe mai in Occidente è un'argomentazione assai convincente sul piano emozionale, un mio caro amico dell'ex- Jugoslavia mi ha assicurato che tale atteggiamento era molto diffuso anche laggiù.

Da: Arrigo Triulzi <arrigo@northsea.sevenseas.org>
Oggetto: Documenti d'identità nazionali

Pur essendo d'accordo su tutto ciò che lei sostiene sull'inutilità dei documenti d'identità nell'ambito della sicurezza, mi permetta di evidenziare un punto debole nella sua argomentazione.

In quanto cittadino italiano, sin dall'età di 14 anni mi è obbligatorio portare sempre con me un valido documento d'identità (o passaporto) ovunque mi sposti sul territorio italiano. Sin da quell'età, la mia carta d'identità è stata controllata una volta soltanto, nel 1991, durante la prima Guerra del Golfo. Fu un'esperienza piuttosto spiacevole, che ha visto protagonisti poliziotti armati con fucili mitragliatori puntati su di me, ed io che venivo sbattuto contro un muro a circa 100 metri da casa; tutto questo per il semplice fatto che ero uscito di casa con un borsone voluminoso e che casa mia si trovava ad essere proprio sopra l'allora consolato americano (che ha poi cambiato sede, così che i controlli di sicurezza più stupidi, rudi e maleducati possono essere fatti ai danni di altri malcapitati, colpevoli del terribile reato che il proprio padrone di casa ha affittato degli uffici agli USA). Naturalmente bisogna anche aggiungere che gli stessi idioti che mi hanno perquisito mi avevano visto passare davanti al loro posto di guardia innumerevoli volte (lo stesso ristretto gruppo di agenti si dava il cambio in turni di quattro unità), e ciò rende quel gesto “autorizzato” dall' “incrementato stato di allerta” ancora più insensato.

A parte questo episodio, ho utilizzato la mia carta d'identità per le seguenti attività: per votare, per attraversare i confini di altri paesi europei, per provare la mia identità in caso di acquisti con assegno o carta di credito sopra una certa cifra, per aprire un conto corrente bancario, e per richiedere altri documenti allo Stato.

Tutto qui: nessuna "interruzione" o "ritardo" dovuti a "continui controlli dei documenti d'identità".

Da: Joao Luis Pinto <jpinto@inescporto.pt>

Oggetto: Documenti d'identità nazionali

Quanto segue è il mio commento al suo articolo "Documenti d'identità nazionali" apparso nel numero di aprile della sua newsletter CRYPTO-GRAM (ottima e interessante):

Io sono favorevole all'idea di un documento d'identità nazionale, a patto che serva unicamente ad autenticare i singoli individui, senza fornire informazioni generiche su di essi.

Vivo in Portogallo. La tendenza europea (ad eccezione del Regno Unito) è quella di permettere e di accettare come un fatto naturale l'esistenza di documenti d'identità nazionali, anche con l'aggiunta di informazioni biometriche. Il problema, specialmente nel mio paese, è che per alcune funzioni specifiche sono richiesti molti altri documenti, fra cui la patente di guida, tessere di Previdenza Sociale, e documenti IRS (l'IRS è l'Imposta sul Rendimento del Singolo individuo, in Portogallo) identificativi, alcuni di questi necessari a dimostrare l'identità in determinate situazioni. In certi casi sono obbligatori molteplici documenti. Questa mancanza di riferimenti incrociati crea svariati problemi. Per esempio, la notifica di un cambiamento di indirizzo deve essere inviata a più di un organo che gestisce l'emissione di questi documenti.

Io credo possibile un unico documento identificativo che sostituisca tutti quelli summenzionati, dotato di riferimenti incrociati con database di informazioni a contesto ristretto.

L'unica funzione di quel documento di identità sarebbe quella di attestare che io sono un unico individuo, con un particolare indirizzo e un particolare numero o codice identificativo. Niente di più, niente di meno. Tutte le altre informazioni dovrebbero risiedere su database dedicati a contesto ristretto, permettendo una semplice impostazione dei privilegi d'accesso alle informazioni (ad esempio l'IRS dovrebbe conoscere solo i miei dati fiscali, non la mia fedina penale). Il documento d'identità, magari abilitato con un sistema tipo smartcard, presenterebbe la mia fototessera, le mie impronte digitali e/o la scansione della mia iride firmate digitalmente dallo Stato, permettendo così una verifica dell'identità sul posto e in presenza della scheda. Il documento d'identità dovrebbe poter fornire poi un certificato digitale firmato da un'Autorità di Certificazione Statale, che dichiarerebbe la mia identità se fosse necessaria una verifica digitale. Naturalmente, questa Autorità di Certificazione dovrà essere creata, e dovrà essere "forte" al massimo quanto gli algoritmi crittografici che le stanno dietro... Ma questo, a mio avviso, è uno scenario sempre migliore di quelli attuali.

Tutto questo andrebbe, credo, a beneficio dell'asserzione di identità, con un impatto che andrà a toccare vari livelli (per esempio la sicurezza delle transazioni web, le frodi ai danni delle carte di credito, e la falsificazione di documenti d'identità). Inoltre sarà un passo importante per ridurre il "divario di impedenza" che esiste fra autenticazione e identità "fisiche" e "digitali/on-line".

Da: Jonathan Bennett <jonathan.bennett@zdnnet.co.uk>

Oggetto: Falla di sicurezza nel protocollo Bluetooth

Scrivo in merito al pezzo sul Bluesnarfing nell'ultimo numero di Crypto-Gram. Anzitutto, squillo di trombe: non è stato il Times a scoprire questa storia. È stato ZDNet UK a trattare dettagliatamente il Bluesnarfing lo scorso febbraio, portando il problema all'attenzione di produttori e politici. Il fatto che

il giornalista autore dell'articolo sul Times abbia cercato di ottenere i dettagli di uno dei nostri contatti non fa che renderlo evidente. Si vedano:

< <http://news.zdnet.co.uk/communications/wireless/0,39020348,39145881,00.htm> > oppure
< <http://tinyurl.com/22ptv> >
< <http://news.zdnet.co.uk/communications/wireless/0,39020348,39145886,00.htm> > oppure
< <http://tinyurl.com/378l6> >
< <http://news.zdnet.co.uk/communications/wireless/0,39020348,39146427,00.htm> > oppure
< <http://tinyurl.com/3ezbv> >

Un altro reporter ed io abbiamo incontrato Adam Laurie e abbiamo assistito ad un'operazione di Bluesnarfing su un telefonino che ci eravamo portati e che perciò eravamo certi che non fosse stato manomesso. Io sono in grado di offrire un po' più di discernimento rispetto all'articolo del Times, in quanto sono giornalista esperto di tecnologia. La vulnerabilità che permette il Bluesnarfing sembra essere un problema di implementazione di certi telefonini. Non ci sono molte prove a sostegno che sia una falla del modello di sicurezza di Bluetooth, e Laurie è d'accordo con questa valutazione. Secondo un altro consulente, il problema risiede nell'implementazione del protocollo object exchange (OBEX) da parte dei costruttori; questo permette all'aggressore di connettersi al telefono, di usare apparentemente un servizio che non richiede autenticazione, e poi di emettere una richiesta verso un servizio che invece richiede autenticazione, aggirando così la sicurezza.

Credo che il Bluesnarfing sia un problema meno grave di quel che Laurie o il Times vorrebbero farvi credere. A differenza di attacchi via Internet, esso richiede vicinanza fisica al bersaglio. Poi, solo certi modelli di cellulare sono vulnerabili, ed è facile per i produttori effettuare una serie di verifiche. Inoltre esiste un rimedio molto semplice: disattivare il Bluetooth. È possibile riattivarlo per quei brevi momenti in cui se ne ha davvero bisogno.

Non si deve poi dimenticare che questa non è l'unica situazione in cui sono a rischio i dati sensibili memorizzati nei telefonini. È molto più probabile che qualcuno dimentichi il cellulare o il PDA sul treno dopo una serata passata a bere. Anche le agende cartacee possono andare smarrite, è successo anche ai reporter. Questo prima ancora di iniziare a pensare ad attacchi di ingegneria sociale. Vi sono altre cose di cui preoccuparsi prima di andare nel panico con il Bluesnarfing.

Abbiamo riportato tale problematica perché crediamo che la gente debba essere informata su queste cose, e così coloro che hanno dati davvero importanti archiviati nei propri cellulari possono premunirsi contro eventuali attacchi. Portare alla luce questo problema causa anche pressioni sui costruttori perché prendano provvedimenti, e in questo senso l'articolo del Times, anche se in ritardo, servirà a qualcosa.

Da: Paul Leeming <paul@leeming.cjb.net>
Oggetto: Serrature autorizzate dalla TSA

Ho appena letto la sua Crypto-Gram in merito alle serrature autorizzate dalla TSA, e il fatto che lei non lo consideri un grosso problema perché "del resto erano già in grado di scassinare le precedenti serrature".

Essendo un ex-pilota di linea, osservo il problema da un'altra angolazione -- che succederebbe se qualcuno senza scrupoli volesse METTERE qualcosa nel vostro bagaglio? Una chiave speciale sarebbe per gli addetti ai bagagli lo strumento perfetto per mettere droga o altro materiale di contrabbando nel vostro bagaglio per poi recuperarlo a destinazione. Voi, quindi, correte il rischio di essere "beccati" con quel materiale illecito, e vi ritrovate incastrati per un reato che non avete commesso. Questo permetterebbe anche a un potenziale terrorista di piazzare un piccolo ordigno NELLA vostra valigetta, e potrebbe plausibilmente scagionarsi, dato che la vostra valigetta era "chiusa a chiave".

Il vero problema a questo punto è che NON SI SA PIÙ se il vostro bagaglio è stato aperto, mentre se manca il vostro lucchetto perché è stato scassinato, è possibile riportare il fatto alle autorità e avviare un'indagine (o almeno creare una traccia cartacea in vostra difesa).

Da: Victor Bogado da Silva Lins <bogado@visgraf.impa.br>
Oggetto: Copertura per targhe

Nell'ultimo numero della sua newsletter Crypto-Gram lei ha parlato di una copertura per targhe automobilistiche che le rende illeggibili da certe angolazioni. Molti brasiliani hanno architettato una soluzione low-tech per lo stesso "problema"... semplicemente attaccano un po' di nastri alla targa o all'auto stessa. Quando la macchina è in corsa (oltre i limiti previsti), i nastri svolazzano intorno e davanti alla targa, rendendo così molto difficile leggerla.

Da: Matthew Rubenstein <email@matruby.com>
Oggetto: Commento di un lettore su "centralizzazione e benefici per la sicurezza"

Drew Johnson le ha inviato un'errata analisi della "sicurezza centralizzata", concludendo erroneamente che "centralizzare è una buona cosa". Il suo primo scenario protegge 10 depositi da 100 dollari ognuno con una "distinta" cassetta di sicurezza il cui scasso costa 200 dollari. Ma le sue cassette sono tutte identiche, quindi si spendono 200 dollari non solo per scassinare la prima di esse, ma tutte e dieci. Per cui egli si trova già una "sicurezza centralizzata", proteggendo 1000 dollari -- con un'unica cassetta che ne vale 200 -- divisi in 10 parti. Pessima strategia. Il suo secondo scenario mette praticamente tutti e 1000 dollari in un'unica cassetta di sicurezza, e stabilisce un costo di scasso aumentato soltanto fino a 500 dollari. Entrambi gli scenari sono centralizzati, entrambi costano meno del valore del premio, entrambi sono insicuri.

Se il sig. Johnson mettesse 100 dollari in 10 *diverse* cassette di sicurezza da 200 dollari, che non cedano *tutte quante* dopo che sono stati spesi i primi 200 dollari per scassinare la prima, egli avrebbe decentralizzato la sicurezza e sconfitto i criminali. Qui abbiamo non solo una lezione di decentralizzazione della sicurezza, ma di sicurezza della policoltura, superiore alla scarsa sicurezza della monocoltura.

Da: "David Nasset, Sr." <david.nasset.sr@iname.com>
Oggetto: Commento di un lettore su "Centralizzazione e benefici per la sicurezza"

Drew ha commesso tre errori, tutti e tre generati dalla sua asserzione: "Tuttavia, dato che i computer su cui si trovano le cassette di sicurezza virtuali hanno le stesse vulnerabilità, lo stesso attacco può essere ripetuto al minimo costo marginale (cioè 1 dollaro)". Infatti, la falla individuata da Drew si applica non ai singoli documenti identificativi, ma solo al documento identificativo nazionale.

Errore n.1: Questa asserzione presume che le serrature siano identiche. Ciò è improbabile perché, come nel caso del documento identificativo, i sistemi saranno probabilmente molto molto differenti. Il circuito MasterCard non utilizza lo stesso sistema di sicurezza del circuito VISA, ed entrambi si servono di un sistema di sicurezza diverso da quello della Motorizzazione Civile dello Stato di Washington, che a sua volta è diverso da quello dell'Immigrazione. Perciò, il mio bancomat, la mia carta di credito, la mia patente di guida e il mio passaporto è improbabile che vengano sconfitti dallo stesso attacco. Solo se il sistema usato è lo stesso, allora lo stesso tipo di attacco funzionerà tutte le volte.

Errore n.2: Anche se le serrature da 100 dollari sono identiche, rimane sempre più remunerativo puntare al premio più grande.

Supponiamo che Drew abbia ragione, e che tutte le serrature da 200 dollari siano le stesse, e che tutte siano accessibili grazie a una vulnerabilità scopribile spendendo 200 dollari e un dollaro soltanto per

exploitarla, ottenendo 100 dollari. L'aggressore quindi sferra dieci attacchi, ottiene 1000 dollari, un profitto di 790 e un aumento del 478% del proprio investimento.

Ora, supponiamo che attacchi la serratura da 500 dollari. Trova un exploit che può usare per 50 dollari ad attacco (anche se 1 dollaro è egualmente probabile). Ora egli attacca le cassette di sicurezza di dieci persone diverse. Quanto spende? 950 dollari. Quanto guadagna? 10.000 dollari, un profitto di 9.050 dollari ovvero un aumento del 1052% del proprio investimento.

Errore n.3: La vulnerabilità descritta da Drew è ancora peggiore se _usiamo davvero_ il documento d'identità nazionale. Se un exploit può essere ripetuto a buon mercato, e siamo tutti prigionieri dello stesso sistema, allora il denaro di ognuno è protetto dalla stessa serratura da 500 dollari.

Drew ha assunto che tutte le serrature da 1 dollaro sarebbero cedute a causa dello stesso exploit, cosa che abbiamo già stabilito essere improbabile. Perciò, un aggressore non può avvalersi dello speciale beneficio di utilizzare lo stesso attacco a poco prezzo in continuazione.

Tuttavia, chiunque si serva della serratura da 500 dollari (documento d'identità nazionale) è _obbligato_ ad usare la _stessa serratura_. Con le altre serrature, esse sono costrette dalle circostanze ad essere spesso differenti e, in molti casi (VISA e di contro MasterCard), la scelta di una serratura è nelle mani di chi la compra. Nel peggiore dei casi, l'aggressore può attaccare tutte le VISA o tutte le patenti di guida dello Stato di Washington, o tutti i passaporti USA. Tuttavia, con i documenti d'identità nazionale, non abbiamo scelta. Un exploit ripetibile che funziona con uno di essi, funzionerà con dieci, cento, mille persone diverse, e quando funziona, permette di prendere _tutto_.

Quindi preferisco rimanere con un sistema dove il peggior exploit prende poco a molti, e io ci perdo poco a mia volta, piuttosto che abbracciare un sistema dove lo stesso risultato significa che tutti perdono tutto ciò che hanno messo al sicuro.

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

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

La versione italiana è curata da Communication Valley SpA <http://www.communicationvalley.it/>.
Per iscriversi o cancellarsi andare all'indirizzo <http://www.cryptogram.it/>.
I numeri arretrati sono disponibili all'indirizzo <http://www.cryptogram.it/>.
Per informazioni crypto-gram@communicationvalley.it.

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

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

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

Copyright (c) 2004 by Bruce Schneier.

