

CRYPTO-GRAM
15 gennaio 2005

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

Edizione italiana curata da Communication Valley SpA

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

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

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

Gli stessi articoli della newsletter sono disponibili sul blog di Bruce Schneier:
<<http://www.schneier.com/blog>>.

** **

In questo numero:

- [Prendere le impronte digitali agli studenti](#)
- [Le ristampe di Crypto- Gram](#)
- [PIN facili da ricordare](#)
- [Disattivare il network GPS](#)
- [News](#)
- [Gli scassinatori e il "sentirsi al sicuro"](#)
- [Le News di Counterpane](#)
- [La sicurezza della scritta HOLLYWOOD](#)
- [Un gruppo di lavoro IT per il programma Secure Flight Privacy](#)
- [La Guerra Cibernetica](#)
- [Commenti dei lettori](#)

** **

Prendere le impronte digitali agli studenti

<http://www.schneier.com/blog/archives/2005/01/fingerprinting_1.html>

Un nuovo trend di sicurezza che si sta sviluppando negli Stati Uniti contempla il tracciamento degli scolari quando salgono e scendono dagli scuolabus. Un distretto scolastico a Spring, nel Texas, utilizza dei badge identificativi per registrare queste informazioni e inviarle poi alle stazioni di polizia via wireless. Un altro distretto scolastico a Phoenix ha messo in atto qualcosa di simile utilizzando dei lettori di impronte digitali. Tale sistema dovrebbe servire a prevenire la perdita di un bambino, sia nel caso di rapimento, sia per cause accidentali.

Che cosa sta succedendo? Questa gente ha forse perso la ragione? Controllare i bambini quando salgono e scendono dagli scuolabus è un'idea semplicemente ridicola. È un sistema costoso, invasivo, e non aumenta molto la sicurezza.

La sicurezza è sempre un compromesso, un bilanciamento. In "Beyond Fear" ho illustrato un procedimento in cinque passi per valutare le misure di sicurezza. L'idea è quella di poter determinare razionalmente se una certa misura di sicurezza vale davvero la pena di essere applicata. Nel mio libro

ho applicato questo procedimento a qualsiasi cosa, dagli allarmi antirapina domestici alle azioni militari antiterrorismo. Proviamo ad applicarlo anche a questo caso.

Passo 1: Quali risorse si sta cercando di proteggere? I bambini.

Passo 2: Quali sono i rischi legati a tali risorse? La perdita di un bambino, che si tratti di rapimento o di cause accidentali. Il rapimento di bambini è un grave problema negli Stati Uniti: le probabilità che un bambino venga rapito da un membro della famiglia sono una su 340, e che venga rapito da un estraneo sono una su 1200 (ogni anno). Queste statistiche sono del 1999 -- si veda il link più sotto -- e comprendono ogni sorta di incidenti che normalmente non verrebbero considerati rapimenti. In più, mi pare ragionevole supporre che i valori a Spring, in Texas, siano molto più bassi. Pochissimi fra quei rapimenti hanno coinvolto scuolabus, perciò non è molto chiaro quanto gravi siano i rischi specifici affrontati con questi controlli.

Passo 3: Quanto bene la soluzione di sicurezza riesce ad attenuare tali rischi? Non molto bene.

Proviamo ad immaginare in che modo questo sistema possa offrire sicurezza nel caso di un rapimento. Se un rapitore (ammettiamo che si tratti di qualcuno che il bambino conosce) sale sullo scuolabus e scende con il bambino alla fermata sbagliata, il sistema registrerà un simile evento. In altri casi, ad esempio se il rapimento è avvenuto prima che il bambino salisse sul pullman o dopo esserne sceso, il sistema non registrerebbe nulla di sospetto. Certo, direbbe agli investigatori se il rapimento è occorso prima del servizio mattutino e prima o dopo il tratto percorso sullo scuolabus, ma questa sola informazione vale l'intero sistema di tracciamento? Ne dubito.

Si potrebbe immaginare uno scenario da film dove questo genere di sistema di controllo possa servire all'eroe per recuperare il bambino rapito, ma non sembra molto utile nel mondo reale.

Passo 4: Quali altri rischi vengono generati da questa soluzione di sicurezza? Il rischio aggiuntivo è rappresentato dai dati raccolti dalla costante sorveglianza. Dove vengono raccolte tali informazioni? Chi ha accesso ad esse? Per quanto tempo rimangono archiviate? Queste sono problematiche di sicurezza molto importanti che non vengono neppure menzionate.

Passo 5: Quali costi e compromessi vengono imposti da questa soluzione di sicurezza? Ce ne sono due. Il primo è ovvio: il denaro. Non ho dati precisi, ma immagino sia costoso produrre per ogni bambino un badge identificativo e installare questo sistema su ogni scuolabus. Il secondo costo è meno tangibile e materiale: si tratta della perdita di privacy. Stiamo crescendo bambini che pensano sia normale che i loro spostamenti quotidiani vengano controllati e registrati dalla polizia. Quel senso di privacy non è cosa a cui rinunciarvi così alla leggera.

Quindi, in conclusione: questo sistema ne vale davvero la pena? No. La sicurezza che si ottiene non vale il denaro speso e la riduzione di privacy. Se l'obiettivo è quello di rendere più sicuri i bambini, i soldi potrebbero essere meglio spesi in altri modi: guardie nelle scuole, programmi educativi per gli alunni, ecc.

Se tale sistema è così insensato, perché viene implementato in almeno due diverse città statunitensi? La risposta ovvia è che i distretti scolastici non hanno riflettuto a fondo sul problema. Potrebbero essere stati sedotti dalla tecnologia, o dalle aziende che hanno costruito il sistema. Ma vi è un'altra, interessante, possibilità.

In "Beyond Fear" parlo del concetto di agenda, ovvero di priorità. Il procedimento in cinque passi visto prima è un'agenda soggettiva, e dovrebbe essere valutata dal punto di vista della persona incaricata di prendere la decisione riguardante il compromesso, il bilanciamento in gioco. Se pensiamo che a prendere tale decisione siano i funzionari scolastici, ecco che improvvisamente il sistema acquista un senso.

Se un rapimento avviene sul territorio scolastico, l'indagine che ne segue potrebbe facilmente danneggiare i funzionari scolastici, che potrebbero persino rischiare il posto. Se vediamo questa

misura di sicurezza come qualcosa che protegge LORO tanto quanto protegge i bambini, allora il tutto viene ad avere un senso. Il compromesso può non valerne la pena in generale, ma vale di sicuro per LORO.

I rapimenti sono un grave problema, e le misure atte a ridurre il rischio sono una buona cosa. Ma ricordiamoci che la sicurezza è sempre un compromesso, un bilanciamento, e che un buon sistema di sicurezza è quello dove i benefici di sicurezza valgono il denaro speso, i vantaggi, e le libertà a cui si rinuncia. Insomma, questo sistema non vale la pena.

La notizia:

< http://news.com.com/In+Texas%2C+28%2C000+students+test+e-tagging+system/2100-1039_3-5456061.html > oppure < <http://makeashorterlink.com/?U65C2173A> >

Statistiche sui rapimenti:

< <http://www.ncjrs.org/pdffiles1/ojdp/196467.pdf> >

** **

Le ristampe di Crypto- Gram

Crypto- Gram è attualmente al suo ottavo anno di pubblicazione. I numeri precedenti coprono tutta una serie di argomenti legati alla sicurezza e si possono trovare tutti a questo indirizzo: < <http://www.schneier.com/crypto-gram.html> >. Quella che segue è una selezione di articoli apparsi in questo mese gli anni scorsi.

Dirottare aerei e Servizi Segreti nazionali:

< <http://www.schneier.com/crypto-gram-0401.html#11> > (originale)

< <http://www.cryptogram.it/gennaio04.htm#a11> > (traduzione)

Prendere le impronte digitali agli stranieri:

< <http://www.schneier.com/crypto-gram-0401.html#3> > (originale)

< <http://www.cryptogram.it/gennaio04.htm#a3> > (traduzione)

I livelli di minaccia terroristica codificati a colori:

< <http://www.schneier.com/crypto-gram-0401.html#1> > (originale)

< <http://www.cryptogram.it/gennaio04.htm#a1> > (traduzione)

L'esercito e la Guerra Cibernetica

< <http://www.schneier.com/crypto-gram-0301.html#1> > (originale)

< <http://www.cryptogram.it/gennaio03.htm#a11> > (traduzione)

Una Underwriters Laboratories in versione cibernetica?

< <http://www.schneier.com/crypto-gram-0101.html#1> >

Code signing:

< <http://www.schneier.com/crypto-gram-0101.html#10> >

Block ciphers e stream ciphers:

< <http://www.schneier.com/crypto-gram-0001.html#Blockbuster> >

** **

PIN facili da ricordare

< http://www.schneier.com/blog/archives/2005/01/easytoremember_1.html >

Il Regno Unito si sta convertendo a un sistema "chip e PIN" per le transazioni della carta di credito. Il passaggio è stato lento, ma entro gennaio (non sono sicuro se per l'inizio o la fine di gennaio) ogni carta di credito britannica sarà una smart card.

Questo genere di sistema esiste già in Francia e altrove. Le carte hanno dei chip incorporati. Quando si vuole procedere a un acquisto, si fa passare la carta in uno slot e si inserisce su un tastierino il proprio codice PIN a quattro cifre. Presumibilmente non verrà mai disattivato il sistema a striscia magnetica più firma, necessario alle carte statunitensi.

Una delle paure del consumatore, riguardo a questo procedimento, è che cosa può succedere se si dimentica il proprio PIN. Per calmare tali paure, le compagnie di carte di credito hanno inserito degli annunci sui giornali suggerendo ai consumatori di cambiare il proprio PIN e di usare un numero facile da ricordare: "Continuate a dimenticare il vostro PIN? È semplice cambiarlo con il sistema chip e PIN. Basta scegliere qualcosa di più facile da ricordare, come una data di nascita o i vostri numeri fortunati".

Ma le compagnie di carte di credito non hanno nessuno che si occupa della sicurezza?

L'annuncio continua dicendo che è possibile cambiare il proprio PIN per telefono, il che porta con sé tutta una serie di ulteriori problemi.

L'annuncio:

< <http://blog.artesea.co.uk/2004/12/389-doh.html> >

(So che non si tratta di una fonte primaria, ma ho ricevuto questa informazione da almeno due lettori, e uno di essi sostiene che l'annuncio sia comparso sul London Times).

** **

Disattivare il network GPS

< http://www.schneier.com/blog/archives/2005/01/shutting_down_t.html >

Il Governo degli Stati Uniti sta considerando la possibilità di disattivare temporaneamente la rete USA di satelliti di posizionamento globale durante un'eventuale crisi nazionale, per evitare che i terroristi sfruttino tale tecnologia a loro vantaggio.

Durante una crisi nazionale, la tecnologia GPS aiuterà i "buoni" molto più di quanto potrà aiutare i "cattivi". Disattivare il sistema porterà quasi certamente più danni che benefici.

Questo mi fa venire in mente i commenti dopo gli attentati di Madrid, secondo cui dovremmo sviluppare dei modi per disattivare la rete di telefonia cellulare dopo un attacco terroristico. Le bombe a Madrid furono detonate usando telefoni cellulari, ma non chiamando telefoni collegati alle bombe. Dopo un attacco terroristico, i telefoni cellulari sono vitali sia per i soccorritori che per i superstiti.

Qualsiasi tecnologia può avere utilizzi positivi o negativi - - automobili, telefoni, crittografia, ecc. Nella maggior parte dei casi occorre accettare dei possibili utilizzi negativi se si vuole sfruttare quelli positivi. E ciò è bene, dato che ci sono molti più "buoni" che "cattivi", e gli usi positivi sono molto maggiori rispetto a quelli negativi.

< <http://www.securityfocus.com/news/10140> >

** **

News

Lo scassinamento di casseforti per lo scienziato informatico:

< <http://www.crypto.com/papers/safelocks.pdf> >

È un ottimo intervento, che ha fatto arrabbiare di brutto la comunità dei fabbri:

< <http://tinyurl.com/3vq2b> >

Si può avere un dibattito ragionevole sul tema “segretezza contro esposizione totale”, ma molti di questi commenti sono semplicemente squallidi. Blaze NON è disonesto. I suoi risultati NON sono banali. Ritengo che la comunità della sicurezza fisica abbia molto da imparare dalla comunità della sicurezza informatica e che quest'ultima abbia a sua volta molto da imparare dalla prima. Il lavoro di Blaze nel campo della sicurezza fisica dà lezioni importanti per la sicurezza informatica e, come si può vedere, anche per la sicurezza fisica, nonostante i tentativi di questa gente di banalizzarla cercando di attaccare Blaze.

Altri worm per telefoni cellulari:

< <http://www.computerworld.com/newsletter/0,4902,98578,00.html?nlid=SEC2> >

oppure < <http://makeashorterlink.com/?T23711A3A> >

Un documento del 1959 che parla di un generatore hardware di numeri casuali collegato a un computer.

< http://phk.freebsd.dk/rc3600/DASK_rng.pdf >

La polizia ha piazzato alcuni esplosivi al plastico nella valigetta di un passeggero preso a caso, come parte di un test per i cani antiterrorismo. Quattro giorni dopo non si aveva ancora traccia degli esplosivi.

< <http://www.msnbc.msn.com/id/6672643/> >

È assolutamente sensato introdurre in un aeroporto una valigetta piena di esplosivo, per testare la sicurezza. Quel che è sbagliato è introdurre l'esplosivo nel bagaglio di qualcuno a sua insaputa e senza il suo permesso; il residuo esplosivo potrebbe rimanere nella valigetta per molto tempo dopo la prova, e potrebbe essere rilevato da uno di quegli spettrometri di massa che registrano il residuo chimico associato agli esplosivi. Ma se dovete inserire degli esplosivi al plastico nella valigetta di un ignaro passeggero, non potreste almeno segnarvi di quale valigetta si tratta?

La Commissione Irlandese sul Voto Elettronico (Irish Commission on Electronic Voting) ha pubblicato un rapporto di 433 pagine. Si tratta di un'analisi eccellente e dettagliata del sistema di voto elettronico acquistato dal governo irlandese.

< http://www.cev.ie/htm/report/download_first.htm >

EPIC ha pubblicato un elenco di Risoluzioni per la Privacy per l'Anno Nuovo.

< <http://www.epic.org/privacy/2004tips.html> >

In una storia su un'anomalia informatica che ha obbligato Comair a cancellare 1.100 voli il giorno di Natale, mi sono state attribuite queste parole dall'Associated Press: “Se questo genere di cose è potuto succedere per sbaglio, che cosa accadrebbe se fosse fatto di proposito dai criminali?” Di sicuro ho detto questo, ma avrei preferito che il reporter non avesse estrapolato questa frase. È la classica istigazione alla paura a cui mi oppongo quando viene usata da altri.

< <http://www.guardian.co.uk/uslatest/story/0,1282,-4696749,00.html> >

Molte uniformi appartenenti agli ufficiali di sicurezza degli aeroporti canadesi sono andate perdute:

< <http://www.cbc.ca/story/canada/national/2004/12/03/airport-security041203.html> > oppure

< <http://makeashorterlink.com/?C64716A3A> >

Ho scritto nel mio blog a riguardo delle implicazioni di sicurezza degli strumenti di autenticazione visiva, come appunto le uniformi:

< http://www.schneier.com/blog/archives/2004/12/canadian_airpor.html >

Una vernice isolante per contenere il traffico Wi-Fi:

< <http://informationweek.com/story/showArticle.jhtml?articleID=56200676> >
oppure < <http://makeashorterlink.com/?N35712A3A> >

Ottima analisi delle implicazioni di sicurezza connesse al non rilasciare patenti di guida agli immigrati clandestini:

< <http://releases.usnewswire.com/GetRelease.asp?id=40902> >

Gli orologi da polso con altimetro sono ora una minaccia terroristica:

< http://www.watchreport.com/2005/01/new_casio_digit.html >

Qualcuno mi spieghi perché dovrei preoccuparmi che un orologio indossato da qualcuno possa essere usato come detonatore. La persona stessa può fungere, e in maniera assai più efficace, da detonatore. E se il rischio è costituito da un ordigno sufficientemente piccolo da entrare in un orologio, allora qui abbiamo problemi ben più grossi che non una particolare marca di orologi.

Lo Honeynet Project ha pubblicato un rapporto in cui si dichiara che Linux non è sottoposto a hacking. I sistemi di prova hanno un'aspettativa di vita media (l'intervallo di tempo prima di venire penetrati con successo) di tre mesi. Questo è molto maggiore rispetto alle macchine Windows, che hanno aspettative di vita medie dell'ordine di pochi minuti. È importante ricordare che questo rapporto si concentra sui sistemi vulnerabili. I ricercatori di Honeynet hanno predisposto circa 20 sistemi vulnerabili per monitorare le tattiche degli hacker, e hanno scoperto che nessuno stava svolgendo dell'hacking a danno di tali sistemi. Questa è la vera notizia: agli hacker, Linux non interessa. Due anni fa, un sistema Linux vulnerabile sarebbe caduto in meno di tre giorni; oggi ci vogliono tre mesi. Perché? A mio avviso, il perché è una combinazione di due motivi. Uno, Linux è di parecchio più sicuro di Windows. Due, gli aggressori si stanno concentrando su Windows: rende di più.

< <http://www.honeynet.org/papers/trends/life-linux.pdf> >

< <http://asia.cnet.com/news/security/printfriendly.htm?AT=39210602-39037064t-39000005c> >

oppure < <http://makeashorterlink.com/?J16724A3A> >

< http://www.techweb.com/article/printableArticle.jhtml;jsessionid=GTAR0EED2ZP4MQSNDBCCCKHSCJ_UMKJVN?articleID=56200327&site_section=700028 > oppure

< <http://makeashorterlink.com/?B27734A3A> >

Questo articolo, intitolato "Border Patrol hails new ID system" [Pattuglia di Frontiera accoglie un nuovo sistema identificativo] si sarebbe potuto più accuratamente intitolare "Nessun terrorista catturato dal nuovo sistema identificativo". Si noti come il terrorismo giustifichi la spesa di questa misura di sicurezza, e come venga poi usata per qualcosa di diverso. Si osservino le cifre relative alle persone incarcerate per i reati più svariati, e si noterà subito quanto insignificanti siano in realtà moltissimi di quegli arresti.

< <http://www.washtimes.com/national/20041220-103705-9177r.htm> >

La triste storia di un falso positivo vittima dell'antiterrorismo:

< <http://www.nzherald.co.nz/index.cfm?ObjectID=3602231> >

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

Gli scassinatori e il "sentirsi al sicuro"

< http://www.schneier.com/blog/archives/2004/12/burglars_and_fe.html >

Questa citazione proviene dal libro "Confessions of a Master Jewel Thief" [Confessioni di un Maestro del Furto di Gioielli] di Bill Mason (Villard, 2003): "Non c'è niente che giochi a favore di un ladro più del sentimento di sicurezza della gente, del loro sentirsi al sicuro. Ecco perché quei luoghi pieni di allarmi e di guardie possono essere a volte i bersagli più facili. Il fattore più importante in ambito di sicurezza -- ancor più delle serrature, degli allarmi, dei sensori, o di guardie armate -- è l'atteggiamento. Un edificio protetto soltanto da una banale serratura a combinazione, ma abitato da persone attente e a conoscenza dei rischi è ben più sicuro di un edificio dotato del sistema d'allarme più sofisticato del mondo i cui inquilini hanno l'idea di vivere in una fortezza inespugnabile."

L'autore, uno scassinatore, ha scoperto che i condomini di lusso erano un ottimo bersaglio. Pur usando molta più tecnologia di sicurezza rispetto ad altri edifici, erano vulnerabili per il semplice fatto che nessuno credeva possibile che un ladro avrebbe potuto superare l'ingresso.

Il libro:

< <http://www.amazon.com/exec/obidos/ASIN/0375508392/counterpane/102-3568437-0872933> >
oppure < <http://makeashorterlink.com/?H58712A3A> >

** **

Le News di Counterpane

Schneier parlerà alla sezione di Boston della CPCU (Chartered Property Casualty Underwriter) il 20 gennaio:
< <http://www.licatakelleher.com/NewsPage.html> >

Counterpane è stata recentemente dichiarata scanning vendor autorizzato sia per il programma SDP (Site Data Protection) di Mastercard, sia per il programma CISP di Visa (Cardholder Information Security Program).
< <http://www.counterpane.com/pr-20050111.html> >

Inoltre, Counterpane ha avuto un ottimo quarto trimestre. Un comunicato stampa a riguardo è imminente.

Breve intervista audio con Schneier:

< http://www.nytimes.com/packages/html/technology/20050112_SCHNEIER_AUDIOSS/double.html >
oppure < <http://makeashorterlink.com/?Z59724A3A> >

** **

La sicurezza della scritta HOLLYWOOD

< http://www.schneier.com/blog/archives/2004/12/physical_access.html >

A Los Angeles, la scritta "HOLLYWOOD" è protetta da una recinzione e da un cancello chiuso a chiave. Dato che svariate agenzie hanno la necessità di accedere alla scritta per scopi diversi, la catena che chiude il cancello è formata da parecchi lucchetti tutti concatenati. Ogni agenzia possiede la chiave del proprio lucchetto, ma non quelle per gli altri lucchetti. Naturalmente, chi può aprire uno dei lucchetti, può di conseguenza aprire il cancello.

Questo è un bell'esempio di un sistema di controllo accessi multiutente. È semplice, e funziona. È possibile complicarlo finché si vuole, con lucchetti differenti, in serie e in parallelo.

** **

Un gruppo di lavoro IT per il programma Secure Flight Privacy

< http://www.schneier.com/blog/archives/2005/01/secure_flight_p.html >

Sto partecipando ad un gruppo di lavoro per aiutare a stabilire l'efficacia e le conseguenze sulla privacy del programma Secure Flight della TSA. Finora abbiamo avuto un solo incontro, e pare proprio che sarà un esercizio interessante.

Per chi non ha seguito queste vicende, il programma Secure Flight è il seguito di CAPPS-I (CAPPS sta per Computer Assisted Passenger Pre-Screening). CAPPS-I è entrato in vigore nel 1997, ed è un semplice sistema che confronta i passeggeri delle linee aeree con una watch list di terroristi. Un seguito a questo sistema, CAPPS-II, è stato proposto lo scorso anno. Un sistema più complicato, che avrebbe assegnato a ogni viaggiatore un "punteggio di rischio" basato su informazioni contenute in database governativi e commerciali. Si è levato un incredibile scalpore da parte del grande pubblico, accusando l'eccessiva invadenza del sistema, ed è stato cancellato durante l'estate. Secure Flight è il nuovo sistema a seguito di CAPPS-I.

Molti di noi credono che Secure Flight sia semplicemente CAPPS-II con un nuovo nome. Spero di sapere presto se ciò corrisponde o meno al vero.

Spero di imparare molte cose su Secure Flight e sul profiling dei passeggeri delle linee aeree, ma probabilmente non potrò scrivere nulla a riguardo. Per poter essere un membro di questo gruppo di lavoro, sono stato obbligato a richiedere un'autorizzazione speciale SEGRETA del governo degli Stati Uniti, e a firmare un NDA, cioè un Accordo di Non Divulgazione, promettendo che non avrei rivelato quelle che sono state definite "Informazioni di Sicurezza Sensibili" (Sensitive Security Information, SSI).

SSI è una delle tre nuove categorie di informazioni segrete, categorie che a mio avviso non dovrebbero esistere. Esiste già uno schema classificatorio (CONFIDENTIAL, SECRET, TOP SECRET, ecc.) e le informazioni dovrebbero rientrare in quello schema, oppure essere di pubblico dominio. Uno schema nuovo crea soltanto confusione. Lo NDA che abbiamo dovuto firmare era molto generico, e comprendeva condizioni come quella che avrebbe permesso al governo di condurre perquisizioni delle nostre residenze senza bisogno di un mandato. (Due sindacati federali hanno minacciato di denunciare il governo per diverse condizioni contenute in quell'NDA, che riguarda anche molti impiegati del Dipartimento di Sicurezza Nazionale. E di recente il Dipartimento di Sicurezza Nazionale ha ritirato l'accusa).

Dopo una respinta da parte mia e di molti altri, ci è stato presentato un NDA molto meno oneroso.

La segretezza che circonda questo gruppo di lavoro non mi piace. Gli NDA e i briefing segreti sollevano problematiche etiche piuttosto serie per le commissioni governative di supervisione. Sospetto che verrò impressionato con una serie di affermazioni segrete e non verificabili che dovrò accettare oppure (più probabilmente) mettere in questione, ma non potrò discuterne con altri. In generale, le deliberazioni segrete favoriscono gli interessi di chi impone le regole. E vanno decisamente contro lo spirito del FACA (Federal Advisory Committee Act).

Ma soprattutto non sono sicuro del perché questo gruppo di lavoro non sia in violazione del FACA. Il FACA è una legge del 1972 intesa a regolare le modalità con cui l'Esecutivo si serve di gruppi di consulenti al di fuori del governo federale. Fra le varie regole, è richiesto che le assemblee consultive annuncino i loro incontri, li tengano in pubblico, e prendano appunti da rendere poi disponibili al pubblico. Quando fu costituito, il Dipartimento di Sicurezza Nazionale ottenne una specifica esenzione dal FACA: il Segretario della Sicurezza Nazionale ha l'autorità di esonerare dal FACA qualsiasi assemblea consultiva; l'unico requisito è che il Segretario notifichi l'assemblea nel Registro Federale. Ho guardato, e non ho visto nessun annuncio o notifica.

A causa dello NDA e del non seguire il FACA, non potrò esercitare appieno i miei diritti del Primo Emendamento. Questo significa che il governo può impedirmi di dire cose che potrebbero essere importanti da sapere da parte del grande pubblico. Ad esempio, se venissi a scoprire che il vecchio programma CAPPS non è stato in grado di identificare dei veri terroristi, o che molte persone che non erano terroristi sono state ingiustamente fatte sbarcare, e il governo ha cercato di non divulgare queste notizie (sto inventando, è solo un esempio), io non potrei dirvi nulla. Il governo potrebbe perseguirmi a seguito dello NDA, perché potrebbe sostenere che questi fatti sono "SSI" (Sensitive Security Information) e il pubblico non verrebbe mai a conoscenza di questi fatti poiché non vi sono obblighi di incontri aperti, come accade invece con le commissioni conformi al FACA.

vecchi. Proprio così, l'unico elemento nuovo è il dominio; sono le stesse cose, che avvengono però in una nuova arena. Ma dato che l'arena del cyberspazio è molto diversa da altre arene, vi sono delle differenze che val la pena prendere in esame.

Una cosa che non è cambiata è che le espressioni si sovrappongono: malgrado gli obiettivi siano diversi, molte delle tattiche usate da eserciti, terroristi e criminali sono le medesime. Così come tutte e tre le categorie utilizzano armi da fuoco e bombe, tutte e tre possono servirsi di attacchi cibernetici. Così come uno scontro a fuoco non è necessariamente un atto di guerra, ogni attacco via Internet portato a termine con successo, non importa quanto implacabile, non è necessariamente un atto di guerra cibernetica. Un attacco cibernetico atto a provocare un collasso della rete elettrica può essere parte di una campagna di guerra cibernetica, ma potrebbe anche essere un atto di terrorismo cibernetico, di crimine cibernetico, o anche (se svolto da qualche quattordicenne che non capisce fino in fondo quel che sta facendo) di vandalismo cibernetico. Quale sia fra questi dipenderà dalle motivazioni dell'aggressore e dalle circostanze intorno all'attacco... proprio come nel mondo reale.

Per trattarsi di guerra cibernetica, deve essere innanzitutto una guerra. E nel XXI secolo, una guerra comprenderà inevitabilmente una guerra cibernetica. Così come la guerra si è spostata nei cieli grazie allo sviluppo di aquiloni e palloni aerostatici prima e di aerei poi, e in seguito la guerra si è spostata nello spazio grazie allo sviluppo di satelliti e missili balistici, la guerra si sposterà nel cyberspazio con lo sviluppo di armi specialistiche, tattiche e strategie di difesa.

Il muovere una guerra cibernetica

Non dovrebbero esserci più dubbi sul fatto che gli eserciti più preparati e meglio pagati del mondo stanno pianificando una guerra cibernetica, sia per quanto riguarda attacco e difesa. Sarebbe stupido da parte di un esercito ignorare la minaccia di un attacco cibernetico e non investire in risorse difensive, o di scartare la possibilità strategica o tattica di lanciare un attacco cibernetico offensivo contro un nemico in tempo di guerra. Se la storia ci ha insegnato che molti eserciti sono davvero stupidi e ignorano la marcia del progresso, la guerra cibernetica è stata trattata in tale misura nelle cerchie militari da non poter essere ignorata.

Ciò implica che almeno alcuni degli eserciti del nostro mondo hanno pronti degli strumenti di attacco via Internet che conservano in caso di guerra. Potrebbero essere dei tool per attacchi denial-of-service. Potrebbero essere exploit che permetterebbero all'intelligence militare di penetrare sistemi militari. Potrebbero essere virus e worm simili a quelli che stiamo vedendo ora, ma forse pensati esclusivamente per una determinata nazione o rete. Potrebbero essere dei Trojan che spiano reti, o che compromettono operazioni di rete, o che permettono a un aggressore di penetrare all'interno di altre reti.

Gli script kiddies sono aggressori che sfruttano codice di exploit scritto da altri, ma che non comprendono a fondo le complessità di quel che stanno facendo. Al contrario, gli aggressori professionisti spendono moltissimo tempo a sviluppare gli exploit: trovando nuove vulnerabilità, scrivendo codice per exploitare, cercando modi per coprire le proprie tracce. I veri professionisti non rilasciano il loro codice agli script kiddies; quel materiale ha molto più valore se rimane segreto fino a quando non serve davvero. Credo che i militari siano in possesso di raccolte di vulnerabilità dei comuni sistemi operativi, di applicazioni generiche, o anche di software militare specifico utilizzato dai loro potenziali nemici, e di codice per sfruttare quelle vulnerabilità. Credo che questi militari stiano tenendo segrete tali vulnerabilità, e che le stiano conservando in caso di guerra o di altre ostilità. Sarebbe irresponsabile da parte loro non farlo.

L'attacco cibernetico più ovvio è la disattivazione di grandi aree di Internet, almeno per un certo periodo. Di sicuro alcuni militari hanno la capacità di farlo, ma in mancanza di una guerra totale, dubito che agirebbero in questo senso: Internet è una risorsa troppo utile e rappresenta una larghissima fetta dell'economia mondiale. Più interessante è il caso in cui volessero provare a disabilitarne dei pezzi a livello nazionale. Se il Paese A andasse in guerra contro il Paese B, il Paese A cercherebbe di disattivare la porzione di Internet del Paese B, o di eliminare i collegamenti fra la parte

di Internet del Paese B e il resto del mondo? A seconda del paese, una soluzione low-tech potrebbe rivelarsi la più semplice: disabilitare ogni genere di cavi sottomarini utilizzati per l'accesso. L'esercito del Paese A potrebbe trasformare la propria Internet in una rete solamente nazionale, se lo volesse?

Per un approccio più chirurgico, possiamo anche immaginare attacchi cibernetici pensati per distruggere le reti di determinate organizzazioni, come ad esempio l'attacco denial-of-service ai danni del sito di Al Jazeera durante il recente conflitto in Iraq, condotto presumibilmente da hacker filo-Americani, ma forse dal governo stesso. Possiamo immaginare un attacco cibernetico contro le reti informatiche del quartier generale dell'esercito di un paese, o contro le reti che gestiscono informazioni logistiche.

Un concetto importante da tener presente è che la distruzione è l'ultima cosa che un militare vuole fare ai danni di una rete di comunicazioni. Un militare vuole solo disattivare la rete nemica nel caso non si ottengano utili informazioni da essa. La cosa migliore da fare è infiltrarsi nei computer e nelle reti nemiche, spiare, e distruggere senza preavviso parti specifiche delle loro comunicazioni al momento opportuno. Un'altra buona cosa da fare è mettersi in ascolto passivo. Dopodiché, un'altra buona cosa è effettuare analisi del traffico: analizzare chi sta parlando a chi e le caratteristiche di tale comunicazione. Solamente quando i militari non possono effettuare nessuna di queste operazioni, prendono in considerazione l'idea di chiudere tutta la rete. Oppure la chiudono nel raro caso in cui i benefici derivanti dal togliere completamente il canale di comunicazione al nemico siano superiori a tutti gli altri vantaggi sopra descritti.

Proprietà della guerra cibernetica

Siccome aggressori e difensori utilizzano lo stesso hardware e software di rete, esiste una tensione fondamentale fra attacco cibernetico e difesa cibernetica. La National Security Agency si è riferita a questo fenomeno chiamandolo "equities issue" (questione di equità) e si può riassumere in questo modo. Quando i militari scoprono una vulnerabilità in un software diffuso, possono avvertire il produttore e far sistemare tale vulnerabilità, oppure non rivelarla. Riparare la vulnerabilità offre un sistema più sicuro sia ai buoni che ai cattivi. Mantenerla segreta significa che i buoni possono sfruttarla per attaccare i cattivi, ma significa anche che i buoni sono altrettanto vulnerabili. Finché tutti si servono degli stessi microprocessori, degli stessi sistemi operativi, protocolli di rete, applicativi software, ecc., la questione di equità sarà sempre tenuta presente nel pianificare una guerra cibernetica.

La guerra cibernetica può assumere aspetti tipici dello spionaggio, e non implica necessariamente la guerra aperta. Nel linguaggio militare, la guerra cibernetica non è necessariamente "calda". Dato che molta parte di un conflitto cibernetico riguarda l'ottenimento del controllo su una rete e il mettersi in ascolto su di essa, potrebbe non esserci alcun danno evidente a seguito di operazioni di guerra cibernetica. Questo significa che le stesse tattiche possono venire usate in tempo di pace da agenzie di intelligence nazionali. C'è un rischio considerevole qui. Proprio come i voli statunitensi U2 sull'Unione Sovietica avrebbero potuto essere visti come un atto di guerra, anche il penetrare deliberatamente all'interno delle reti informatiche di un paese può essere considerato allo stesso modo.

Gli attacchi cibernetici mirano alle infrastrutture. In questo non sono diversi dai normali attacchi militari contro altre reti: energia elettrica, mezzi di trasporto e di comunicazione, ecc. Tutte queste reti vengono utilizzate sia dai civili che dai militari, in tempo di guerra, e gli attacchi sferrati a tali infrastrutture danneggiano entrambi. Ad esempio, quando gli Alleati bombardarono i ponti ferroviari tedeschi durante la Seconda Guerra Mondiale, ciò influì sul trasporto civile e militare. Quando gli Stati Uniti hanno bombardato i link di comunicazione durante la Prima e la Seconda Guerra in Iraq, ciò ha influito sulle comunicazioni civili e militari. Gli attacchi cibernetici, persino queglii attacchi mirati con tanta precisione come le attuali bombe intelligenti, possono avere con tutta probabilità degli effetti collaterali.

Gli attacchi cibernetici possono essere usati per muovere una guerra di informazione. La guerra di informazione (information war) è un altro argomento che ha ricevuto parecchia attenzione da parte dei media ultimamente, anche se non è un concetto nuovo. Lanciare volantini sui soldati nemici per convincerli ad arrendersi è guerra di informazione. Trasmettere programmi radiofonici alle truppe nemiche è guerra di informazione. Visto che le persone ottengono sempre più informazioni attraverso il cyberspazio, esso diventerà sempre più teatro di guerra di informazione. Non è difficile immaginare attacchi cibernetici progettati per scegliere i canali di comunicazione del nemico e utilizzarli come veicolo di guerra di informazione.

Dato che la guerra cibernetica prende di mira l'infrastruttura di informazioni, essa può risultare molto più dannosa per quei paesi che hanno un'imponente infrastruttura informatica. L'idea è che un paese tecnologicamente povero possa decidere che un attacco cibernetico tale da influire a livello mondiale, influirebbe in maniera sproporzionata sui propri nemici, poiché le nazioni più ricche si affidano a Internet molto di più di quelle povere. Per certi versi questo è il lato oscuro della linea di demarcazione digitale, e uno dei motivi per cui paesi come gli Stati Uniti sono così preoccupati per ciò che riguarda la difesa cibernetica.

La guerra cibernetica è asimmetrica, e può essere un attacco di guerriglia. A differenza delle offensive militari convenzionali, che coinvolgono intere divisioni di uomini e mezzi, gli attacchi cibernetici vengono portati avanti da alcuni operatori addestrati. In questo modo, gli attacchi cibernetici possono essere parte di una campagna bellica di guerriglia.

Gli attacchi cibernetici sono degli efficaci attacchi a sorpresa. Per anni abbiamo sentito terribili avvertimenti di un possibile "Pearl Harbor elettronico". Queste cose sono in larga parte iperboliche oggi. Ne parlo più approfonditamente in quell'articolo sul terrorismo cibernetico apparso su un precedente numero di Crypto-Gram, ma in questo momento posso dire che, semplicemente, l'infrastruttura non è vulnerabile a sufficienza in quel senso.

Gli attacchi cibernetici non hanno necessariamente un'origine ovvia. A differenza di altre forme di guerra, l'indicazione sbagliata è più una prerogativa di un attacco cibernetico. È possibile subire dei danni senza sapere da dove proviene l'attacco. Questa è una differenza significativa; c'è qualcosa di terrificante nel non conoscere il proprio avversario -- o di credere di conoscerlo, e scoprire di avere torto. Pensate se gli Stati Uniti, dopo Pearl Harbor, non avessero saputo chi li aveva attaccati?

La guerra cibernetica è un bersaglio mobile. Nel paragrafo precedente ho detto che oggi i rischi di un Pearl Harbor elettronico sono infondati. È vero, ma questo, come tutti gli altri aspetti del cyberspazio, è un qualcosa in continuo cambiamento. Le miglierie tecnologiche influiscono su tutto e tutti, compresi i meccanismi di attacco cibernetico. E Internet sta diventando cruciale per una parte sempre maggiore della nostra infrastruttura, rendendo più attraenti gli attacchi cibernetici. Verrà un tempo, in un futuro forse non tanto remoto, in cui un attacco cibernetico a sorpresa diventerà una minaccia realistica.

Infine, la guerra cibernetica è un concetto dalle molte sfaccettature. È parte di una campagna militare più ampia, e gli attacchi possono avere componenti reali e cibernetiche. Un esercito potrebbe prendere di mira l'infrastruttura di comunicazione del nemico attraverso attacchi veri e propri (bombardamenti di determinate strutture di comunicazione e di cavi di trasmissione) e attacchi virtuali. Una campagna di guerra di informazione potrebbe comprendere il lancio di volantini, l'usurpazione di un canale televisivo, e l'invio in massa di messaggi e-mail. Molti attacchi cibernetici hanno ancora degli equivalenti non cibernetici più semplici da attuare: un paese che volesse isolare il collegamento a Internet di un altro paese, potrebbe trovare una soluzione a bassa tecnologia, per esempio la sottomissione di compagnie come la Cable & Wireless; più facile da realizzare che non sviluppare un worm o virus mirato. La guerra cibernetica non sostituisce la guerra vera e propria, è soltanto un'altra arena in cui la guerra più grande viene combattuta.

La gente enfatizza i rischi della guerra e del terrorismo cibernetici. È un argomento attraente e concentra l'attenzione dei media. Allo stesso tempo, le persone minimizzano i rischi del crimine cibernetico. Oggi il crimine è un grosso business su Internet, e si ingrandisce sempre più. Ma

fortunatamente le difese sono le medesime. Le contromisure mirate alla prevenzione da attacchi di guerra o di terrorismo cibernetici saranno efficaci anche contro il crimine e il vandalismo cibernetici. Per cui, anche se le organizzazioni renderanno sicure le proprie reti per i motivi sbagliati, faranno ugualmente la cosa giusta.

Il mio precedente intervento sul terrorismo cibernetico:
< <http://www.schneier.com/crypto-gram-0306.html#1> >

** **

Commenti dei lettori

Da: "David Allsopp" <d.allsopp@signal.QinetiQ.com>
Oggetto: Il profiling basato sull'analisi comportamentale

L'ultima volta che ho preso un aereo, ho sentito una passeggera (Europea, di razza bianca) raccontare come era stata fermata e perquisita ai checkpoint una volta, e poi ancora, e ancora, e ancora finché aveva perso le staffe con un ufficiale di sicurezza e li aveva accusati di molestia. Il problema pareva dovuto al fatto che la signora fosse diventata nervosa ai checkpoint dopo essere stata controllata la prima volta. Così era stata fermata una seconda volta a causa di "ansietà immotivata", rendendola ancora più nervosa la terza volta, e così via.

Se da una parte sono d'accordo con quanto lei afferma, secondo cui degli esseri umani addestrati rappresentano una sicurezza migliore, è altresì difficile saper distinguere la paura di volare dalla paura di essere fermati (per l'ennesima volta) e dalla paura di essere presi.

Da: Jimmy Stiefel <jimmy@gigagig.org>
Oggetto: Il profiling basato sull'analisi comportamentale

Nella sua disamina sull'analisi comportamentale, lei ne evidenzia i vantaggi rispetto ad altre forme di profiling, e in generale ritengo che la sua analisi sia azzeccata (come sempre). Tuttavia, sono rimasto un po' sorpreso che lei abbia abbozzato e non abbia messo in discussione il record di "successi" del programma dell'aeroporto Logan ("Il programma in vigore al Logan Airport ha già catturato 20 persone che si trovavano nel paese illegalmente o che avevano mandati di cattura pendenti delle specie più varie").

Sono dell'idea che queste "catture" potrebbero rappresentare più facilmente dei danni collaterali che non veri e propri successi del programma. Sono falsi positivi - - persone con scheletri nell'armadio che le hanno fatte agire in maniera sospetta nei pressi della sicurezza. Ma erano terroristi? È stato sventato qualche complotto? Siamo tutti di conseguenza più sicuri? Credo che la risposta sia no.

Un immigrato clandestino rappresenta una minaccia di sicurezza per i voli nazionali? Un individuo con un mandato pendente rappresenta una minaccia? Di sicuro i sistemi computerizzati di controllo dei passeggeri sono specificamente impostati per rilevare queste tipologie di minaccia percepita. Questo è esattamente il genere di persone che finiscono negli "elenchi", e lei ha ampiamente spiegato perché non si tratta di misure di sicurezza efficaci. Catturare una *minaccia* perché agisce in modo sospetto è una buona cosa. Catturare una non-minaccia perché agisce in modo sospetto è un falso positivo.

Mi delude il fatto che lei non abbia sottolineato questo. Catturare un immigrato clandestino è un problema dell'immigrazione, non della sicurezza dei trasporti. In assenza di ulteriori dettagli, questi sono stati fallimenti, e non successi, del programma. Alcune persone hanno perso la propria libertà a causa di tali fallimenti.

Per me, tutto ciò è "mission creep". È un'erosione dei nostri diritti civili. Ricordiamoci che lo scopo della sicurezza negli aeroporti è quello di farci viaggiare sicuri, non quello di valutare gli scheletri

nell'armadio di ogni passeggero. Questo è un costo nascosto del programma, un costo che ogni cittadino dovrà sostenere.

Da: Richard Barrell <rbarrell@sentryware.com>
Oggetto: La sicurezza dell'Aeroporto di Israele

Mi sembra che lei si sia dimenticato di spiegare la parte più importante della tecnica di controllo della sicurezza dell'Aeroporto di Israele. La parte fondamentale è che gli ufficiali di sicurezza (gli "aggressori") lavorano in gruppi, e i "difensori" sospettati verranno interrogati due volte da ufficiali diversi, che poi confronteranno i loro appunti.

Questo significa che il "difensore" non soltanto deve tenere a mente una storia complessa, ma deve anche sottostare a una seconda raffica di domande, le risposte alle quali verranno confrontate con le risposte date nel corso del primo interrogatorio.

Questo doppio cieco è un sistema efficace per scovare incongruenze nella storia di un "difensore", ed è anche un procedimento che avviene in pubblico, aumentando così la pressione su eventuali aspiranti terroristi.

Da: Paul Schumacher <psch@optonline.net>
Oggetto: La sicurezza dell'Aeroporto di Israele

Questa è una cosa di così tanto tempo fa che non ricordo i dettagli. Nell'Esercito fui istruito su come eludere le domande di un inquisitore.

Il trucco non sta nell'aver costruito una buona storia di copertura, ma di adattare una storia vera all'occasione. Nell'esempio di un interrogatorio all'aeroporto:

Domanda: Dove si sta recando?

Risposta: In Pakistan. (Questa è la destinazione del volo, per cui è ovvio).

D: Chi conosce laggiù?

R: George Hamilton (Semplicemente cambio il nome di Osama Bin Laden con il nome di un altro).

D: Come ha incontrato questa persona?

R: Durante il periodo di addestramento base dell'Esercito (un campo di addestramento di Al Qaeda per l'Esercito di Allah).

D: Che cosa stava facendo laggiù?

R: Imparavo a diventare un soldato (quello che per un uomo è un terrorista per un altro può essere un combattente per la libertà).

Come può vedere, ho raccontato molte cose "vere" secondo una certa prospettiva, ma una storia completamente falsa se osservata da un altro punto di vista. Piegando uno schema che esiste nella realtà per creare una "verità alternativa", si dovrebbe riuscire a sostenere anche un difficile interrogatorio.

Da: "Charlie Brooks" <linux@HBCS.Org>
Oggetto: Mettere i CD nel microonde

Lei ha scritto: "Il modo migliore per distruggere i CD-R è quello di metterli nel microonde e impostare il forno sul massimo per cinque secondi".

Una volta ho dato un party il cui tema era "esperimenti molto sciocchi da fare con un forno a microonde", perché mi trovavo in possesso di un microonde che nessuno voleva. Ho chiesto ai partecipanti di portare qualsiasi cosa volessero far saltare, e devo dire che la creatività dei miei amici era tale da sbalordire. Molti portarono dei CD.

Io (e parecchi miei ospiti, purtroppo) abbiamo imparato a nostre spese che NON SI DEVONO respirare i gas prodotti da CD sottoposti a microonde!

Dato che il diffusore dei raggi di un microonde è una ventola piuttosto efficace, è davvero impossibile evitare l'esposizione ai fumi se ci si trova in uno spazio circoscritto (come una cucina, o la veranda sul retro di casa mia). Una potente ventola di sfogo che muove l'aria verso l'esterno (non una di quelle che si usano oggi, mediocri e che ributtano l'aria nella stessa stanza) potrebbe servire se la ventola posteriore del forno a microonde si trovasse vicino a quella di sfogo.

Forse non dovrebbe consigliare di mettere i CD nel forno a microonde senza aggiungere che così facendo si libereranno dei gas nocivi. La buona notizia è che malgrado la ripetuta esposizione a quei gas, ci siamo tutti ripresi dopo un paio di settimane.

Da: David Jefferson <d_jefferson@yahoo.com>

Oggetto: Le macchine per il voto elettronico

Nel sostenere che si dovrebbe mantenere segreto il codice sorgente delle macchine per il voto elettronico, Jeremy Epstein ha scritto: "Primo, se dobbiamo avere dei tracciati su carta verificabili dall'utente (o qualsiasi sinonimo da lei usato), allora non importa quel che fa il software. Se non funziona a dovere, possiamo individuare l'errore in fase di secondo conteggio".

Purtroppo questo non è affatto vero. Vi sono PARECCHI attacchi di codice maligno che non possono essere rilevati o corretti da nessun confronto fra i tracciati su carta verificabili dall'utente (VVPAT) e le copie elettroniche del voto. Per fare un esempio facile, si tenga presente che un codice maligno che sistematicamente e di nascosto fa in modo di rivelare il voto di una persona al prossimo votante attraverso un segnale segreto sullo schermo, non può essere rilevato usando i VVPAT.

Oppure, se vogliamo usare un esempio più complesso, consideriamo un attacco sferrato casualmente, e per una piccola percentuale del tempo totale delle elezioni, che registri un voto per il Candidato A prescindere da chi il votante era intenzionato a votare; ma che poi mostri chiaramente il voto sbagliato sia sulla schermata riassuntiva, sia sulla copia cartacea prima che il voto sia confermato. Se il votante non si accorge dell'errore, e conferma il voto, allora l'attacco ha successo e il Candidato A ottiene un voto che non avrebbe dovuto avere, e il problema non è rilevabile perché il tracciato cartaceo e i registri elettronici concordano. Se il votante si accorge dell'errore, annulla la scheda cartacea, e torna indietro per correggere il voto; il sistema registra correttamente il voto la seconda volta, sia sulla copia a video che su quella cartacea, e ancora una volta i tracciati elettronici e cartacei concordano, mentre il votante si allontana pensando di essere stato forse lui stesso a commettere lo sbaglio all'inizio. In ogni caso, tutto questo avviene nella privacy della cabina elettorale dove nessun altro può vedere, e anche un votante sospettoso non potrà dimostrare il problema perché non può votare una seconda volta, e perché l'attacco non compare sistematicamente, ma solo per una piccola percentuale del tempo totale.

Se da un lato il tracciato su carta verificabile dall'utente è essenziale, dall'altro non si tratta certo di una panacea: non è semplicemente in grado di rilevare tutti gli attacchi. Non esiste una valida alternativa ad una seria revisione del codice, anche se persino quella è profondamente difficile, e non si ha comunque la certezza che essa rilevi la presenza di codice maligno all'interno del sorgente.

A: Thomas Stalzer <electroemporium@yahoo.com>

Oggetto: Le macchine per il voto elettronico

Lei ha descritto il sistema di voto cartaceo presente in Italia. Esso è in larga parte identico alle schede cartacee usate negli Stati Uniti -- se non oggi, di certo 25 anni fa, cioè l'ultima volta in cui ho vissuto in una circoscrizione che aveva schede cartacee. Esistevano schede diverse per diversi uffici, erano codificate a colori, ecc. E certamente, entrambe le parti partecipavano al conteggio dei voti -- io ero uno scrutatore del partito che avevo scelto.

È tuttavia importante capire come questo procedimento abbia dei propri difetti e rischi. A parte i soliti (riempire le urne di voti fraudolenti, registrazioni fraudolente, doppio voto, e simili), vi sono alcuni rischi meno palesi. Il primo risiede nella precisa definizione di ciò che costituisce un voto valido. Non ricordo la legge del North Carolina in proposito (lo stato dove vivevo quando ero scrutatore); nello stato di New York qualche anno prima la legge richiedeva due linee, che dovevano toccarsi o incrociarsi all'interno del riquadro, per scegliere un determinato candidato. Questo comprende il classico segno di spunta o la X; e comprende anche tutta una serie di altre forme geometriche. Naturalmente, la legge si occupava anche di cose come il votare per più candidati. E trattava anche il caso di segni estranei sulla scheda, cioè quelli al di fuori dei riquadri. Domanda: che cosa bisognerebbe fare con quelle schede che presentano segni di voto *non validi* (ad esempio, una sola riga) in un riquadro, ma un segno di voto corretto in un altro riquadro? Non ricordo che cosa dicesse la legge in proposito, ma le istruzioni del partito erano chiare: contestare qualsiasi scheda dubbia che potesse costituire un voto a vantaggio agli avversari, perché gli altri avrebbero fatto la stessa cosa. I concetti di "valido" o "non valido" non sono così distinti come si vorrebbe; ogni partito cercava di apportare qualche vantaggiosa "correzione". Presumibilmente tutto finiva con il controbilanciarsi...

Ma esiste una problematica più sottile, che ho potuto scoprire quando ho sentito i politici locali dirsi contrari al suggerimento di utilizzare macchine per il voto: le schede cartacee lasciano trapelare informazioni. Ad esempio, ricordo una gara elettorale in cui bisognava votare per tre o sei candidati al consiglio comunale. (La gara era nominalmente non-partisan). Gli schemi di scelta dei tre candidati che venivano indicati sulle schede elettorali rappresentavano un'informazione molto utili per i politici professionisti della città. I sistemi di voto meccanici a leva non registrano simili informazioni; le macchine per il voto elettronico possono farlo o meno. Se a uno interessa quel tipo di analisi, val la pena porre la domanda. Si noti che, anche se il quotidiano locale non riporta questi dati, i voti e tutte le informazioni su di essi sono (negli Stati Uniti) di dominio pubblico; svariati partiti politici potrebbero controllare tutto questo per conto proprio. Questa si può considerare o meno una minaccia, ma bisogna essere consapevoli dell'eventuale fuga di informazioni.

La morale qual è? La sicurezza non è un singolo elemento, che siano schede cartacee, macchine per il voto meccanico o elettronico, tracciati su carta verificabili dall'utente, o altro. È la proprietà di un sistema, e questo comprende il processo di registrazione, di voto, e di conteggio finale.

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

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

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

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

CRYPTO-GRAM è realizzata da Bruce Schneier. Schneier è l'autore dei best seller "Beyond Fear", "Secrets and Lies" [tradotto in Italia col titolo "Sicurezza Digitale"] e "Applied Cryptography", e inventore degli algoritmi Blowfish, Twofish e Yarrow. È il fondatore e CTO di Counterpane Internet

Security, Inc., e membro del comitato consultivo dell'Electronic Privacy Information Center (EPIC). Scrive spesso e tiene conferenze in merito alla sicurezza informatica e alla crittografia. Il suo sito Web è all'indirizzo <<http://www.schneier.com>>.

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

Copyright (c) 2005 by Bruce Schneier.