

CRYPTO-GRAM
15 febbraio 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.

** **

In questo numero:

[Verso una sorveglianza totale](#)

[La politicizzazione della sicurezza](#)

[News](#)

[Le News di Counterpane](#)

[Novità sul libro](#)

[Identificazione e sicurezza](#)

[Le ristampe di Crypto-Gram](#)

[Il Canile: i client di posta elettronica](#)

[L'economia dello Spam](#)

[Commenti dei lettori](#)

** **

Verso una sorveglianza totale

Il mese scorso la Corte Suprema ha permesso al Dipartimento di giustizia di arrogarsi il diritto di arrestare segretamente i residenti privi di cittadinanza. Questo, unito al potere del governo di nominare i prigionieri stranieri "combattenti nemici", così da ignorare i trattati internazionali che ne regolano l'incarcerazione, e unito al potere di trattenere a tempo indeterminato cittadini americani senza alcuna imputazione e privandoli della possibilità di servirsi di un avvocato, fa sembrare gli Stati Uniti sempre più uno stato di polizia.

Dall'11 settembre 2001 in poi, il Dipartimento di Giustizia ha richiesto (e in gran parte ricevuto) poteri aggiunti che gli permettono di operare un livello di sorveglianza sui cittadini americani e sui visitatori mai visto prima. Il Patriot Act degli Stati Uniti, approvato in fretta e furia dopo l'11 settembre 2001, ha dato inizio a tutto questo. In dicembre, una clausola si è trasformata in una legge di stanziamento (Appropriation Bill) che 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, senza alcun mandato -- poiché vengono fatte tutte rientrare nella categoria "istituzioni finanziarie". A partire da quest'anno, il governo degli Stati Uniti sta fotografando e prendendo le impronte digitali dei visitatori provenienti da tutto il mondo ad eccezione di 27 nazioni.

La litania prosegue. Quest'anno verrà attivato CAPPS-II, l'enorme sistema computerizzato del governo atto a verificare le informazioni su tutti i passeggeri delle linee aeree. Il Total Information Awareness, un progetto che avrebbe dovuto collegare vari database e permettere all'FBI di raccogliere informazioni su ogni cittadino americano, è stato bloccato a livello

federale dopo una grandissima protesta da parte dell'opinione pubblica, ma sta proseguendo a livello statale grazie a finanziamenti federali. Durante Capodanno l'FBI ha raccolto i nomi di 260.000 persone che alloggiavano negli alberghi di Las Vegas. Sempre più, ad ogni livello della società, lo stile di sorveglianza totale alla "Grande Fratello" sta pian piano diventando una realtà.

La sicurezza è fatta di bilanciamenti. Non ha senso chiedersi se un certo sistema di sicurezza sia efficace o meno -- altrimenti tutti indosserebbero giubbotti antiproiettile e se ne starebbero rinchiusi nelle proprie case. La domanda più appropriata da porsi è se questi compromessi e bilanciamenti valgono lo sforzo oppure no. Il livello di sicurezza raggiunto vale quanto è costato dal punto di vista economico, delle libertà, della privacy, della convenienza?

Si tratta di una decisione personale, una decisione grandemente legata alla situazione. Per molti i giubbotti antiproiettile non valgono i costi e la scomodità, per alcuni i sistemi d'allarme domestici sì. Molti altri chiudono le porte a chiave durante la notte.

Lo stesso vale per il terrorismo. Occorre ponderare ogni singola contromisura di sicurezza. La sicurezza aggiunta contro i rischi ne vale i costi? Vi sono rimedi più intelligenti per i quali investire i nostri soldi? Come si può paragonare il rischio del terrorismo rispetto ai rischi presenti in altri aspetti delle nostre vite (incidenti stradali, violenza domestica, inquinamento industriale, ecc.)? Vi sono dei costi che sono semplicemente troppo alti da sostenere da parte nostra?

Purtroppo è raro assistere a questo livello di discussione informata. In pochi ci ricordano di quanto minore in realtà sia il rischio del terrorismo. Raramente si parla di quanto l'identificazione delle persone abbia poco a che vedere con la sicurezza, e di come la sorveglianza estesa e generalizzata non serva a molto per evitare il terrorismo. Che fine ha fatto il dibattito sulla questione se siano più importanti le libertà personali e civili che hanno reso grande l'America oppure una qualche sicurezza temporanea?

Invece, il Dipartimento di Giustizia (coadiuvato da una mentalità fortemente "poliziesca" all'interno dell'Amministrazione) sta dirigendo i cambiamenti politici del nostro paese in risposta ai fatti dell'11 settembre e sta realizzando dei compromessi e dei bilanciamenti partendo da una prospettiva assolutamente soggettiva, da cui ne trae benefici anche se causano danni ad altri.

Dal punto di vista del Dipartimento di Giustizia, una supervisione giudiziaria è inutile e ingiustificata; sbarazzarsene è un compromesso migliore. Credono che raccogliere informazioni su tutti sia una buona idea, perché sono meno coinvolti nella perdita della privacy e della libertà. Per loro, una sorveglianza a caro prezzo e sistemi di data mining sono un ottimo bilanciamento, poiché avere più budget significa avere ancora più potere. Secondo la loro prospettiva, la segretezza è preferibile all'apertura; se le forze di polizia sono completamente degne di fede, allora non c'è niente da ricavare da un processo pubblico.

Se si affida la sicurezza alla polizia, i compromessi e i bilanciamenti che faranno risulteranno in misure che ricordano uno stato di polizia.

Tutto questo è sbagliato. I compromessi sono ben più grandi dell'FBI o del Dipartimento di Giustizia. Come un'azienda non incaricherebbe mai un solo dipartimento della gestione del budget, qualcuno al di sopra della ristretta prospettiva del Dipartimento di Giustizia deve bilanciare i bisogni del paese e prendere decisioni in merito a tali compromessi di sicurezza.

Le leggi che circoscrivono i poteri delle forze dell'ordine sono state varate per proteggerci dagli abusi della polizia. La privacy ci protegge dalle minacce di governi, industrie e singoli individui. La forza più grande della nostra nazione deriva dalle nostre libertà, dalla nostra apertura, dai nostri privilegi, e dal nostro sistema giudiziario. Una volta Ben Franklin disse: "Chi rinunciarebbe ai propri privilegi fondamentali per una sicurezza temporanea non merita né

Un buon articolo sull'esternalizzazione della sicurezza informatica:

<<http://www.computerworld.com/networkingtopics/networking/story/0,10801,89100,00.html>> oppure <<http://tinyurl.com/22ybs>>

Un'altra truffa legata alla posta elettronica. Questa fa leva sulla paura del terrore, e su una vulnerabilità Microsoft (vecchia di un mese) che oscura i veri URL.

<<http://www.cnn.com/2004/TECH/internet/01/26/email.scam/index.html>>

Un'operazione di hacking all'interno del Congresso. Pare che alcuni membri del partito Repubblicano si siano introdotti in un gruppo di computer dei Democratici e abbiano avuto accesso a file confidenziali per quasi un anno, a volte passando informazioni alla stampa.

<http://www.boston.com/news/nation/articles/2004/01/22/infiltration_of_files_seen_as_extensive/> oppure <<http://tinyurl.com/25pny>>
<<http://www4.law.cornell.edu/uscode/18/1030.html>>

Ho letto molte persone chiedersi il perché questo non sia un secondo Watergate. Il caso Watergate fu così clamoroso perché le direttive provenivano direttamente dal Presidente. Da allora i politici hanno imparato a non lasciare in giro certe prove. Vi è sempre un buon numero di subalterni a far da capro espiatorio quando vengono alla luce questi episodi. A pensarci bene, è di per se stessa una misura di sicurezza.

Un interessante furto di tipo informatico ai danni di una banca in Israele. Qualcuno ha installato un dispositivo di rete wireless su uno dei rack della banca, e poi lo ha utilizzato per ottenere un accesso clandestino al sistema. Credo che una cosa del genere sia l'inizio di una nuova serie di crimini informatici.

<<http://www.math.org.il/post-office.html>>
<<http://www.math.org.il/post-office2.html>>

Imbrogliare durante un'esercitazione di sicurezza in una centrale nucleare. Quello che segue è il pezzo forte: "Capisco come venga percepito tutto questo, ma il fatto è che non c'è nulla di sbagliato in quel che è accaduto," ha detto Burleson, il dirigente della Wackenhut. "Se avessimo fallito l'esercitazione non sarebbe stato un problema, visto che si aspettavano un nostro fallimento".

<<http://www.sunherald.com/mld/sunherald/news/nation/7807680.htm>>

Costantemente mi capita di vedere stime sui costi di worm e virus, e tutte le volte si tratta di totali invenzioni. Questa è la stima più notevole mai redatta: secondo la BBC, MyDoom è costato 26,1 miliardi di dollari. Mi domando quale azienda antivirus si sia inventata una cifra così assurda.

<<http://news.bbc.co.uk/1/hi/technology/3449931.stm>>

Trend Micro stima che i costi di tutti i virus del 2003 ammontino a 55 miliardi di dollari.

<http://news.com.com/2102-7349_3-5142144.html>

C'è ancora qualcuno che crede a queste cifre?

Una guida alla gestione degli incidenti informatici prodotta dal NIST:

<<http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf>>

Sicurezza attraverso l'oscurità nelle scuole pubbliche:

<<http://www.washingtonpost.com/wp-dyn/articles/A7022-2004Feb2.html>>

Uno studio evidenzia delle vulnerabilità nelle macchine per il voto elettronico:

<<http://www.wired.com/news/print/0,1294,62109,00.html>>

<<http://tn01.com/usatoday/sbct.cgi?s=906902457&i=932220&m=1&d=5392237>>

Il rapporto di RABA:

<http://www.raba.com/press/TA_Report_AccuVote.pdf>

<<http://www.epic.org/privacy/voting/mdvote1.04.pdf>>

Altri problemi con le macchine per il voto elettronico:

<http://verifiedvoting.org/article_text.asp?articleid=997>

Ottimo elenco di risorse sull'economia della privacy:

<<http://www.heinz.cmu.edu/~acquisti/economics-privacy.htm>>

Un'interessante storia di sicurezza ad una frontiera internazionale. Ecco un ottimo assaggio: "La prossima volta in cui vi viene chiesto di fare quasi uno spogliarellino in un punto di controllo a raggi X di un aeroporto (via scarpe, giacca, cintura, portafogli), tenete presente la legge dei rendimenti decrescenti. Siamo probabilmente al punto in cui il mondo potrebbe raddoppiare i propri investimenti in controlli sui viaggi aerei senza ottenerne un guadagno sensibile, tranne per chi offre servizi di sicurezza".

<<http://globeandmail.ca/servlet/story/RTGAM.20040129.wlethome0129/BNStory/Front/>>

oppure <<http://tinyurl.com/3h4kx>>

La watch list statunitense per il terrorismo ha raggiunto i 5 milioni di nominativi:

<<http://www.canoe.ca/NewsStand/TorontoSun/News/2004/01/20/318488.html>>

"La biometria non potrà rilevare i terroristi 'usa e getta'". Un efficace giro di parole, vero?

<<http://www.benadorassociates.com/article/1336>>

Servizi di sicurezza in outsourcing e come avere successo in questo campo (Counterpane viene menzionata).

<<http://www.computerworld.com/networkingtopics/networking/story/0,10801,89100,00.html>>

oppure <<http://tinyurl.com/2tkj6>>

Divertenti storie sulla sicurezza. Le persone sono ancora l'anello debole della catena.

<<http://www.computerworld.com/printthis/2004/0,4814,88303,00.html>>

Solo il 10% dello spam è conforme alla nuova legge USA. Mi sorprende che sia un valore così elevato.

<<http://www.eweek.com/article2/0,4149,1441763,00.asp>>

Lo scorso mese ho parlato dei jammer usati da Musharraf per evitare i bombardamenti. Questo articolo sostiene che gli USA stiano utilizzando la stessa tecnologia in Iraq.

<http://seattletimes.nwsourc.com/html/nationworld/2001847947_jammers31.html>

oppure <<http://tinyurl.com/ytqb9>>

Un articolo interessante sul black-out di agosto nella Costa Orientale degli USA, e su come vi abbia contribuito una vulnerabilità software precedentemente sconosciuta:

<<http://www.securityfocus.com/news/8016>>

Il GAO ha pubblicato un rapporto estremamente interessante sul programma CAPPS-2 per il controllo dei passeggeri delle linee aeree. Secondo questo rapporto, la Transportation Security Administration ha fallito nel far fronte alle perplessità sollevate dal Congresso in merito al programma medesimo, compreso il suo eventuale conformarsi al Privacy Act.

La pagina di EPIC sul tracciamento dei profili dei passeggeri delle linee aeree:

<<http://www.epic.org/privacy/airtravel/gao-capps-rpt.pdf>>

Il mio intervento sullo stesso tema:

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

Cerchiamo di riportare alle giuste dimensioni tutti questi miti, uno per uno. In primo luogo, verificare che un individuo sia in possesso di un documento di identità con fototessera è una misura di sicurezza completamente inutile. I terroristi dell'11 settembre avevano tutti un documento del genere con sé. Alcuni di quei documenti erano autentici, altri contraffatti. Alcuni erano documenti autentici con nomi falsi, comprati a mille dollari cadauno da un impiegato corrotto della Motorizzazione Civile in Virginia. Su Internet sono disponibili patenti di guida fasulle per tutti i cinquanta stati, sufficienti ad ingannare chi non le esamina con attenzione. Oppure, se non volete acquistare documenti di identità online, basta chiedere dove trovarli a qualunque teenager.

Documenti identificativi più difficili da contraffare non aiutano granché, perché il problema non è verificare che questi documenti siano autentici. Questo è il secondo mito dei controlli identificativi, ovvero si crede che l'identificazione, combinata con il tracciamento di un profilo, possa essere un indicatore di intenzione.

L'obiettivo è individuare in qualche modo i pochi "cattivi" sparsi nella vasta moltitudine dei "buoni". In un mondo ideale, ciò che vorremmo è un qualche tipo di ID che indichi l'intenzione. Vorremmo che ogni terrorista portasse una scheda con scritto "malfattore" e tutte le altre persone una scheda con scritto "persona onesta che non cercherà di dirottare aerei o di far saltare in aria alcunché". Allora sì che la sicurezza sarebbe semplice. Basterebbe guardare i documenti identificativi della gente e, se ci imbattessimo in malfattori, non li faremmo imbarcare su un aereo o entrare in un edificio.

Ovviamente tutto ciò è ridicolo, per cui ci si affida all'identità come sostituto. In teoria, se sappiamo chi sei, e se abbiamo informazioni sufficienti su di te, possiamo in qualche modo prevedere se tu possa essere potenzialmente un malfattore o meno. Questo è quanto sta alla base di CAPPS-2, il nuovo sistema governativo di tracciamento profili dei passeggeri delle linee aeree. Le persone vengono suddivise in due categorie basate su svariati criteri: l'indirizzo del viaggiatore, lo storico dei crediti, la documentazione penale e fiscale; la partenza e la destinazione del volo; se il biglietto è stato acquistato in contanti, con assegno, o carta di credito; se il biglietto è di sola andata o di andata e ritorno; se il viaggiatore è solo o in comitiva; con quale frequenza il viaggiatore si imbarca; e quanto tempo prima della partenza è stato acquistato il biglietto.

Il tracciamento di un profilo presenta due modalità di fallimento entrambe pericolosissime. La prima è evidente. Lo scopo della creazione di profili è quello di dividere le persone in due categorie: quegli individui che possono essere dei malfattori e che occorre scremare con maggiore attenzione, e persone che molto difficilmente risultano essere malfattori e che possono venire scremate meno attentamente. Ma un sistema del genere non potrà che creare una terza categoria, molto pericolosa: i malfattori che non rientrano nel profilo.

Timothy McVeigh (il dinamitardo di Oklahoma City), John Allen Muhammed (il cecchino di Washington), e molti dei terroristi dell'11 settembre non avevano precedenti collegamenti con il terrorismo. Unabomber insegnava matematica a Berkeley. I Palestinesi hanno dimostrato che possono reclutare dei kamikaze che non abbiano precedenti in attività contro Israele. Anche i dirottatori dell'11 settembre hanno agito in modo da presentare un profilo assolutamente innocuo: frequent flyer, uno storico di viaggi in prima classe, ecc. I malfattori possono anche effettuare furti di identità, e impossessarsi del profilo di una persona onesta. Il tracciamento di profili può effettivamente produrre meno sicurezza, offrendo a certi individui un sistema facile per aggirare i sistemi di sicurezza.

Ma c'è un'altra modalità di fallimento di questi sistemi, ancor più pericolosa: la categoria delle persone oneste che rientrano nel profilo del malfattore. Dato che i malfattori veri e propri sono così rari, quasi tutti coloro che corrisponderanno al profilo risulteranno essere un falso allarme. Questo non soltanto è uno spreco di risorse investigative che sarebbero meglio impiegate altrove, ma danneggia gravemente quegli innocenti che corrispondono al profilo sbagliato. Che sia qualcosa di semplice come "guidare + persona di colore" o "volare + nazionalità araba" o di

terza si obbligherebbe il mittente a pagare per la posta che invia. Gates ritiene che questa sia la tecnica più promettente per eliminare lo spam una volta per tutte.

Lo spam è un problema interessante, perché è di ordine economico. Lo spam è predominante perché -- per strano che sembri -- è remunerativo. Se non lo fosse, non ce ne sarebbe.

Gates ha ragione di affermare che il modo migliore per affrontare il problema sia quello di cambiarne l'economia. Se gli spammer dovessero pagare per ogni messaggio, così come avviene per chi invia pubblicità cartacea, sarebbero molto meno invasivi. Invierebbero soltanto pubblicità interessanti ed efficaci. Dato che lo spam è quasi gratuito, anche quei messaggi che presentano possibilità di risposta bassissimi creano profitto.

Oggi, un account che genera spam viene chiuso molto velocemente. O almeno, i maggiori ISP bloccano le e-mail che partono da quegli indirizzi. In tutta risposta, gli spammer tendono ad usare account rubati per inviare spam, e tendono a cambiare quegli account molto di frequente e sono disposti a pagare per degli exploit che permettano di penetrare nei sistemi in maniera più efficace.

Questo significa che la sicurezza anti-spam basata sull'identificazione non avrà modo di funzionare. Vorrà dire che ancora più spam si appoggerà ad account rubati. Cambieranno le strategie degli spammer, ma non la quantità di spam. I destinatari di un messaggio e-mail potrebbero decidere di accettare posta solo da persone che già conoscono (le cosiddette "white list"), ma soluzioni del genere sono disponibili e possono funzionare oggi. La maggior parte della gente vuole ricevere e-mail da persone dalle quali non si aspettano e-mail, perciò in molti non si servono delle white list. Richiedere un'identificazione più rigorosa non cambierà molto le cose.

I "puzzle computazionali" sono un'idea interessante, che sta girando da un po' di tempo nella comunità per la sicurezza. L'idea di fondo è la seguente: Alice manda un'e-mail a Bob. Il computer di Bob risponde con un rompicapo matematico che deve essere risolto dal computer di Alice. Il computer di Alice risolve il puzzle e invia la soluzione al computer di Bob, che quindi inoltra la posta a Bob.

È semplice vedere come questo sistema gestisca lo spam. Il computer di Alice non ha problemi a risolvere il puzzle, ma occorre del tempo. Se il computer di Alice deve risolvere milioni di rompicapi al giorno, non sarà in grado di farlo e lo spam viene ridotto.

È una soluzione di tipo economico: rende più costoso l'invio di e-mail. Gli spammer risponderanno penetrando in molti più account e inviando meno spam da ognuno di essi. Ritengo perciò che non vi sarà una riduzione consistente del fenomeno spam.

La terza soluzione proposta da Gates è quella più direttamente economica: richiedere un pagamento per l'e-mail. Anche di questa soluzione si è parlato a lungo nella comunità per la sicurezza. Si tratta anche di una soluzione difficile da attuare. Applicare una struttura di pagamenti sopra l'attuale sistema di circolazione della posta elettronica sarà molto complicato. Dovrà fare i conti con il fatto che lo spam proviene da tutti i paesi del mondo e non soltanto da quelli più economicamente avanzati. La soluzione migliore è quella di raccogliere i pagamenti all'altezza del mittente (in modo che lo spam non vada ad intasare la rete), ma la soluzione più facile sarà quella di raccogliere i pagamenti al livello del destinatario. Tutti dovremo abbandonare l'idea che l'e-mail sia qualcosa di gratuito.

Ma nemmeno questa soluzione risolverà necessariamente il problema di quegli spammer che si impossessano di account di posta altrui. Occorrerà aggiungere altri controlli all'interno della rete: quante e-mail una persona può inviare al giorno, le tariffe massime da applicare, cose del genere. Ancora una volta si tratta di qualcosa di molto difficile da attuare in pratica. Ma almeno si sta riflettendo nella giusta direzione.

questo caso, se il malfattore sa che utilizzerete dei jammer, non dovrà nemmeno preoccuparsi del detonatore; gli basterà impostare un valore soglia abbastanza alto e la vostra apparecchiatura di jamming farà da detonatore.

Da: "John Faulkner" <J.Faulkner@etc.unsw.edu.au>
Oggetto: Il Presidente Musharraf e i jammer radio

Non c'è alcun mistero sul jammer utilizzato per proteggere la scorta di Musharraf dal recente attentato, e non c'è motivo di tenerlo segreto. Si è trattato di un jammer per telefonini GSM (telefoni cellulari, per i nordamericani); questi jammer vengono usati in tutto il mondo da agenzie governative di sicurezza, a seguito dell'adozione praticamente universale dello standard GSM.

Pare che l'ordigno sia consistito in cinque pacchi da 50 chili di esplosivo posizionati in modo da far crollare la parte centrale del ponte, e collegati da un dispositivo di controllo centrale, probabilmente un modem GSM o un telefono con modem. Non dev'essere stato un compito semplice o rapido predisporre tutto questo. Gli ufficiali di polizia che dovevano sorvegliare il ponte hanno giustificato la loro assenza attribuendola alle pessime condizioni meteorologiche.

L'uso di un telefono cellulare fa pensare ad al-Qaeda o ad uno dei suoi alleati. Il camion-bomba usato da Jemaah Islamiah nel suo attacco al nightclub "Sari" a Bali, in Indonesia, nel 2002, fu innescato da un telefono cellulare. Questo è l'esempio più famoso, ma in Asia si sono verificati altri incidenti molto simili.

I telefonini sono un'ottima scelta per chi ha intenzioni dinamitarde. Li si trova dovunque e sono molto poco appariscenti. L'infrastruttura di supporto è già implementata. La trasmissione di innesco viene persa nell'oceano di comunicazioni innocenti. L'utilizzo di una SIM prepagata rende virtualmente irrintracciabile il colpevole.

I modem GSM si trovano facilmente e vengono utilizzati su vasta scala per monitorare i processi industriali. Ad esempio, ogni distributore automatico in Australia ne ha uno. Sono protetti da password e si può comunicare con essi via SMS (messaggi di testo). Di solito possono accendere o spegnere istantaneamente qualsiasi dispositivo collegato, oppure anche in un momento prestabilito, grazie al loro calendario/orologio incorporato. Possono utilizzare la loro porta RS-232 per la ricezione e l'invio di dati seriali.

Se ottenere un modem GSM lascia troppe tracce in giro, si può usare un telefono con modem, come quello usato a Bali. Il modello che si dice sia stato utilizzato in questa occasione possiede un modem incorporato in grado di rispondere ai comandi Hayes (AT) ed ha una porta RS-232. È un modello molto diffuso e di facile reperimento.

I segnali GSM sono, tuttavia, molto suscettibili ad operazioni di jamming poiché, come altre forme di radio segnali digitali, occorre raggiungere una certa soglia segnale/rumore. I telefoni GSM campionano i segnali della stazione trasmittente più vicina per verificare che superino questa soglia. In caso contrario, il telefono si spegne. Quando è operativo, un jammer trasmette un segnale che va ad interferire con il canale di controllo. Questo fa abbassare il coefficiente segnale/rumore di ogni telefonino GSM all'interno del raggio d'azione del jammer. Di conseguenza il telefono si disattiva temporaneamente.

Una volta passato il veicolo su cui è collocato il jammer, il telefono GSM installato nell'ordigno si ricollega con la base e scarica eventuali messaggi SMS in attesa. In questo caso, il messaggio consisteva nel comando di detonazione, ma ecco che viene ricevuto troppo tardi per costituire un pericolo per il bersaglio. Questo spiega il motivo per cui la bomba è esplosa alcuni secondi dopo il passaggio del corteo.

Le reti mobili negli USA si servono di un misto di vecchie tecnologie e di WCDMA (Wideband Code Division Multiple Access) con una minima penetrazione GSM. Ciò non rende gli USA immuni da un simile attacco. Al contrario, questo miscuglio di tecnologie rende solo più difficile ricorrere a misure precauzionali.

In particolare, il WCDMA è ben noto per la propria immunità verso il jamming e pare che questa sia la tecnologia prescelta per sostituire il vecchio sistema analogico statunitense; tecnologia che verrà imposta in Iraq dagli USA. L'esistenza di jammer GSM è un esempio dei benefici di uno standard globale. Per una vulnerabilità conosciuta, esiste una risposta conosciuta, e i jammer erano disponibili sin da quando apparvero i primi telefoni GSM.

Da: <alexcole@verizon.net>

Oggetto: Il Presidente Musharraf e i jammer radio

Un'altra spiegazione possibile della storia di Musharraf: gli ufficiali pakistani della sicurezza potrebbero aver scoperto e disattivato l'ordigno attraverso canali di intelligence, e hanno pubblicato la storia nel tentativo di proteggere la vita della loro fonte di informazioni.

Da: "WJK" <wjk@corvetsys.com>

Oggetto: Una nuova truffa ai danni delle carte di credito

Ma perché non ha rivelato una qualche contromisura per questo tipo di attacco alle carte di credito? La "vittima" potrebbe stare al gioco del truffatore e fornire false informazioni in merito ai numeri sul retro della carta.

Alla fine della telefonata, la "vittima" potrebbe telefonare alla compagnia della carta di credito e allertare la sezione frodi, in modo che controlli questa carta. Nel frattempo, per sicurezza, si potrebbe richiedere un'altra carta.

Il vantaggio di una simile azione è che la frode avrebbe potuto essere intercettata dal negoziante successivo e si sarebbe interrotta molto presto. Invece, senza nessun tipo di reazione positiva, la truffa continua e sia i negozianti che i possessori di carta di credito vengono danneggiati. Qualsiasi persona esperta del ramo potrebbe essere un ottimo contributo per catturare questi ladri, perché di ladri si tratta.

Da: "Clive Robinson" <crobb235@hotmail.com>

Oggetto: Dirottare aerei e i Servizi Segreti nazionali

Vivo e lavoro a Londra, e la "cancellazione dei voli da parte dell'FBI" ha fatto veramente notizia nel Regno Unito, e la BBC ne ha parlato ripetutamente in televisione. (È stato detto solo in un secondo momento che si è trattato di una decisione presa dalla British Airways, su consiglio del governo britannico che a sua volta aveva ricevuto informazioni dall'FBI).

Durante un telegiornale, il conduttore ha specificatamente domandato al giornalista all'aeroporto di Heathrow se "la cancellazione aveva qualcosa a che vedere con l'opposizione dei piloti della British Airways agli ufficiali di volo". La risposta è stata un semplice "non so", ma il tono di voce tradiva un'estrema incertezza.

In un altro programma, il conduttore ha chiesto direttamente ad un politico inglese se gli Stati Uniti stessero gridando "al lupo", e la risposta non è stata prevedibilmente molto convincente, specialmente quando questi ha cercato di spiegare che la minaccia era originata da una donna che avrebbe ingoiato un ordigno prima di imbarcarsi.

Un'opinione già espressa più volte sostiene che i terroristi sappiano come "tirare le corde dell'FBI" e fornire deliberatamente delle informazioni di intelligence fuorvianti, in modo da innescare delle reazioni automatiche da parte dell'FBI. Secondo questo punto di vista, ogni volo cancellato è una vittoria propagandistica per i terroristi, nella guerra dell'informazione. Pur essendo vera quest'ultima osservazione, dubito della prima, dato che fornire una qualsiasi informazione di intelligence all'avversario è estremamente pericoloso per i terroristi, perché offre una traccia (seppur tenue) che porta a loro.

Chiacchierando con un amico che sta in Francia, egli mi ha riferito di come la reazione francese sia stata differente. Pare che un reporter francese abbia notato che nessun aereo americano sia stato colpito e che non vi erano prove credibili di alcuna minaccia. Sembrerebbe che il reporter abbia successivamente fatto notare che forse gli USA stavano cercando di dare il via a uno stato di guerra economica ai danni dell'Europa facendo apparire a rischio le linee aeree non americane, così che chi viaggia per affari sia portato a scegliere vettori americani. Cercando di sdrammatizzare, il mio amico mi ha fermato e mi ha detto che di recente gli USA hanno avuto un comportamento un po' sciocco per quanto riguarda l'acciaio, le banane, e adesso la BSE.

Ho l'impressione che in Inghilterra il supporto alla "guerra al terrore" lanciata dagli USA sia sempre stato marginale anche fra i politici. Ad ogni modo, la notizia secondo cui un uomo si è imbarcato su un volo negli USA con cinque cariche di munizioni in tasca e che queste cariche siano state rilevate solo al suo arrivo nel Regno Unito, ha forse ridimensionato le cose al punto che la sicurezza statunitense viene ora ritenuta incompetente ed inefficace.

Nel resto dell'Europa, il punto di vista su questa vicenda è molto meno amichevole, nella misura in cui si vede questa guerra portata avanti da un "incompetente mai eletto che cerca di portare l'America fuori da una recessione".

I piloti della British Airways che si oppongono alla presenza di ufficiali di volo, lo fanno basandosi su due argomentazioni piuttosto sensate:

1. Un'arma che fosse sicura da usare su un aereo, sarebbe troppo poco potente per avere effetto contro qualcuno che indossa un giubbotto protettivo (questi oggetti, fra l'altro, sono fatti di Kevlar e ceramica, e non vengono rilevati dalla maggioranza dei metal detector e dai sistemi di sicurezza a raggi X). Di conseguenza, una pistola è solo una minaccia per i passeggeri e per l'equipaggio, e i terroristi già lo sanno.

2. Distribuzione di responsabilità. Secondo la legge internazionale, il pilota è responsabile dell'aereo e dei passeggeri. È improbabile che un ufficiale di volo abbia ricevuto un adeguato addestramento per comprendere appieno quale condotta potrebbe mettere a rischio l'aereo, e in caso di emergenza difficilmente si rimetterebbe al giudizio del pilota, anche se avesse tempo per consultarsi.

Inoltre un politico inglese (che avrebbe dovuto avere più buonsenso) ha cercato di mettere sul ridere la faccenda degli "ufficiali di volo" tentando di mettere a segno qualche punto politico. Egli ha detto che dagli USA proviene troppo gergo incomprensibile, ma l'illusione risiedeva nell'affermare che i Texas Rangers giocherebbero a fare gli eroi su tutti i voli diretti negli USA.

In generale, ritengo che le misure di sicurezza degli USA hanno sortito un effetto assai negativo sulla credibilità degli USA fuori dagli USA, e che tutto questo finisca col danneggiarli. Forse sarebbe ora che le agenzie con tre lettere riconsiderino le modalità con cui stanno agendo ultimamente, prima che i danni siano irreparabili.

Da: Steve Loughran <steve_loughran@hpl.hp.com>
Oggetto: Dirottare aerei e i Servizi Segreti nazionali

Lo scopo del terrorismo è diffondere il terrore, solitamente nella (errata) convinzione che questo obblighi l'avversario a cambiare certi aspetti del proprio comportamento. Da un lato atti fisici di terrorismo sono il sistema principale per ottenere un simile obiettivo, dall'altro, se si può diffondere il terrore senza correre alcun rischio, allora tanto meglio.

L'IRA era solita comportarsi così qui nel Regno Unito; vi fu un periodo nel 1993 in cui presero ad attaccare punti delle infrastrutture stradali (come il raccordo Staples Corner M1/North Circular a nord di Londra). Dopo qualcuno di questi attacchi, a volte telefonavano alla stampa, fornivano alcune parole chiave che li identificavano, e facevano il nome di qualche importante raccordo autostradale. Il risultato finiva con l'essere il caos totale dei trasporti, dato che la polizia non faceva altro che chiudere la principale spina dorsale del paese. L'IRA non aveva piazzato alcun ordigno, ma non era possibile esserne certi senza controllare. Così il paese si ritrovava con le strade bloccate, senza alcun rischio per i membri dell'IRA. Terrorismo senza sforzi o rischi: tutto quel che serve è un telefono a pagamento e sapere come reagiranno le forze dell'ordine. Ancora meglio, dato che i finti attacchi possono andare in porto senza perdite di vite umane, non si incorre in dubbi morali da parte di chi ti supporta (in questo caso, tutti coloro che dagli USA hanno inviato denaro per sostenere "la causa", la popolazione di Crossmaglen, la Contea di Armagh, ecc.).

Il che mi porta alle linee aeree. Se tutto quel che occorre per portare un certo livello di scompiglio è fare in modo che il governo intercetti una telefonata in cui si parla di un certo volo, o di una città, e che vi sia la parola chiave "bomba", allora basta fare telefonate simili e fare in modo che siano intercettate. Oppure si possono prevedere quali criteri verranno usati nel tracciamento dei profili dei passeggeri, e comprare biglietti di sola andata sotto nomi sospetti -- e senza alcuna intenzione di presentarsi.

Non so se al-Qaeda abbia già adottato simili strategie (forse la fede nella gloria del martirio ha nascosto alle menti di quella gente le gioie del sopravvivere), ma viste le reazioni esagerate di questi governi con stati d'allarme arancioni, non mi stupirebbe se iniziassero ad usare una tale tecnica.

Da: Mike Stay <staym@clear.net.nz>

Oggetto: Cryptogram: MS Word e le protezioni con password

Eric Thompson di AccessData più di dieci anni fa ha scritto un programma per invertire quel particolare valore hash dei file di MS Word; Microsoft, invece, non ha mai modificato quella protezione. Esiste una funzionalità quasi identica in Excel, e con le stesse vulnerabilità. Io ho scritto quasi tutti gli altri password cracker che si trovano qui:

<http://www.accessdata.com/Product00_Overview.htm#Modules>.

Dei 50 elencati, più della metà funzionano esattamente come l'attacco descritto su SecurityFocus; se si sovrascrivono alcuni byte con un editor esadecimale, viene eliminata la protezione con password, ed è possibile ripristinarla altrettanto facilmente.

Da: Paul Schumacher <psch@optonline.net>

Oggetto: La Sicurezza può essere il miglior alleato del Terrorismo

Avendo lavorato nello Psyops (stato di guerra psicologica) nell'esercito diversi anni fa, ho imparato molto sull'uso strategico della psicologia. Uno dei miei programmi riguardava i granchi di terra e di come strappavano la carne dalle ossa da quei marinai naufraghi troppo deboli per fuggire dalla spiaggia. La notte in cui questo comunicato venne inoltrato a un battaglione di Marines di stanza sulle spiagge di Viquez, infestate dai granchi di terra, nessuno dei soldati dormì per molto.

Il punto è che il vero bersaglio del terrorismo è la mente della vittima, non il suo corpo o i suoi beni. Come una forma perversa di jujitsu, la stessa sicurezza che implementiamo per proteggerci da attacchi terroristici può venire usata come elemento fondamentale dell'attacco.

Per esempio, gli aeroporti hanno cani e dispositivi per rilevare le emissioni chimiche degli esplosivi. Se io prendessi un piccola boccetta di profumo a spray e la riempiessi di nitrobenzene (usato nei solventi per la pulizia interna delle armi da fuoco) per poi spruzzarlo sui bagagli dei passeggeri in attesa di essere esaminati ai punti di controllo, l'intero aeroporto verrebbe presto chiuso grazie alla minaccia percepita dallo staff della sicurezza. Oppure, se spruzzassi i posti a sedere dei luoghi di ristoro o del ristorante dell'aeroporto, i cani anti-bomba diventerebbero cani anti-sedere, con estremo imbarazzo da parte della sicurezza. Una cosa del genere, pur suscitando ilarità, getterebbe parecchio discredito sulle forze di sicurezza.

Con queste azioni sono riuscito a terrorizzare e insieme a danneggiare il pubblico. Ho impedito alla gente di partire in orario e ho ricordato loro di quanto siano vulnerabili al terrorismo. Ho screditato le forze di sicurezza facendole reagire, in modo appropriato, ad una situazione di minaccia, ma non percepita come tale dal pubblico. Come potevano sapere che il mio spray si trattava soltanto di un attacco terroristico fisicamente innocuo, e non di un diversivo per coprire un vero attacco? Intanto ho attaccato e terrorizzato le menti di tutte le persone coinvolte.

Da: Tim Goudy <packrat42@earthlink.net>
Oggetto: Cabine elettorali e telefonini con fotocamera

Nel numero del 15 gennaio, uno dei suoi lettori, Andrew Odlyzko, ha scritto: "La cabina elettorale offre sì un certo livello di protezione contro corruzione e costrizioni, ma solo se riusciamo a far in modo che al suo interno non vengano usati dei cellulari con fotocamera!". Con ciò si implica che i cellulari con fotocamera possano far aumentare i rischi di corruzione e costrizioni offrendo al corruttore un mezzo per verificare che un voto sia stato dato secondo le loro imposizioni. Ma questo non è affatto un rischio significativo.

Consideriamo una situazione ipotetica: Alice sta recandosi al seggio per votare. Sulla strada viene avvicinata da Bob, che intende corromperla e indurla a votare per un certo candidato. Alice dovrà inviare a Bob un'immagine della scheda compilata scattata con il suo telefonino, in modo che Bob possa verificare che lei abbia seguito le istruzioni. Nella riservatezza della cabina elettorale, Alice compila la scheda come specificato da Bob, la fotografa, e invia l'immagine a Bob. In seguito, Alice avvicina un impiegato del seggio e dice: "Scusi, ma ho sbagliato a compilare la mia scheda. Me ne servirebbe un'altra, grazie". Alice quindi vota il candidato di sua preferenza e in più riceve il denaro da Bob. Il rischio che Bob scopra tutto questo è minimo, dato che non c'è modo di collegare Alice ad un certo voto, una volta consegnata la scheda.

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

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.